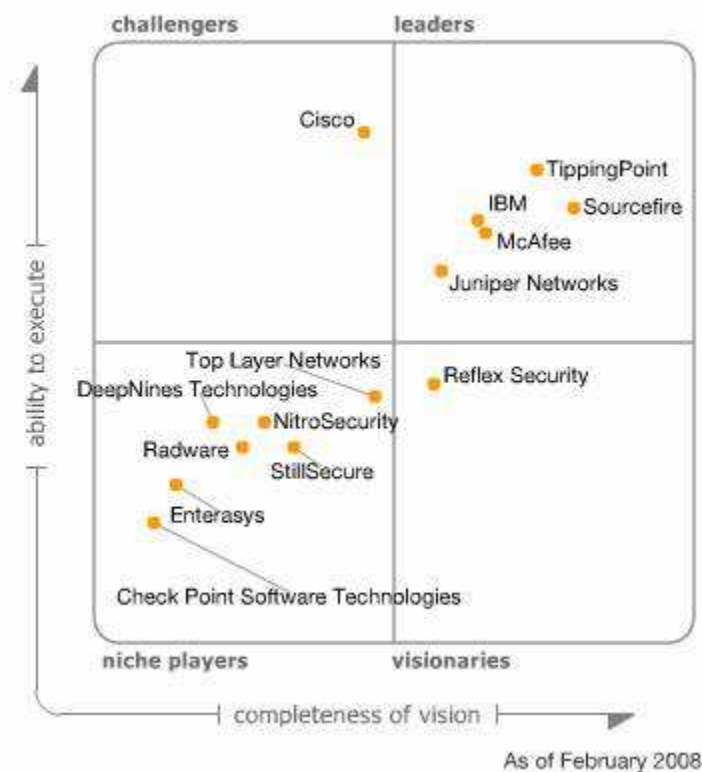




Operaciones Integradas, S.A. de C.V.
Gladiola 317 B. Col Las Margaritas
52165. Metepec, Méx.
Tel: +52 722 2173030
Fax: +52 722 2173030 ext. 4038
Web Site: www.operacionesintegradas.com.mx
Email: staff@operacionesintegradas.com.mx

Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08



Source: Gartner (February 2008)

Market Overview

The network IPS market is the successor technology to the IDS market. IPS contains all the detection features of IDS, with two critical areas of improvement:

- Intrusion prevention moves beyond simple attack signature detection to add vulnerability-based signatures and nonsignature detection capabilities.



- Network IPS sensors operate at wire speeds to enable in-line automated blocking and attack handling. Essentially, network IPS adds "block attacks and let everything else through" security enforcement to the "deny everything except that what is explicitly allowed" policy enforcement that first-generation firewalls provide.

Although the market for separate network IPS and firewall devices will continue through at least 2008, most next-generation firewalls (NGFWs) will use common processing engines to support both functions in one product, even if there is limited interaction between the two products.

The network IPS market for stand-alone appliances continues to grow, from more than \$700 million in 2006 to a forecast \$1 billion in 2007 (see "Forecast: Intrusion Prevention Systems, Worldwide, 2005-2011"). In 2007, there were challenges for market leaders, with Sourcefire off to a bumpy start with its initial public offering (IPO), Internet Security Systems working to integrate into IBM, and TippingPoint running into potential barriers to the acquisition of 3Com by Bain and Company and Huawei to foreign interests (see "Sale of 3Com Could Be Facilitated by TippingPoint Spinoff").

Firewall vendors have been lethargic in improving their in-the-firewall IPS offerings, enabling the stand-alone IPS market to expand faster than it would with competition from firewall vendors. This is mostly because the update cycles for firewalls and IPS appliances have been out of sync, but as enterprises look to replace first-generation IPS units, vendors with integrated capabilities have an opportunity to grow at the expense of stand-alone IPS vendors.

When enterprises compare products, signature quality remains the most weighted and competitive factor on shortlists. Most vendors employ some form of external vulnerability research as an input to signature creation. Some vendors, however, repurpose the open source Snort engine and/or signatures, or other third-party signatures, resulting in problems such as late or inaccurate signatures (owing to poor translations or failure to accommodate the detection signatures in an IPS role), or constraints in innovation, as they potentially must follow the technology direction of Snort. Vendors that invested in their own primary vulnerability research, detection engines and signature creation fared best in our evaluation. Sourcefire owns the copyright on the Snort license, putting the vendors that re-use Snort at a competitive disadvantage, because they can be seen as subordinating themselves to a competitor's road map and a potentially more-restrictive future license under Snort 3.0.

The nature of the most damaging attacks on businesses has changed. Financially motivated attacks don't simply go after unpatched PCs and servers; they increasingly are using targeted malware that requires more than simple, signature-based detection. IPS vendors have not made major advances in detecting and blocking these advanced attacks. Although there has been some increase in "zero day" attacks (which take advantage of computer security holes with no solutions), zero-day signatures, which are signatures for vulnerabilities not yet publicly disclosed, remain controversial.

The risk of reverse-engineering signatures has led vendors that support these signatures to better obfuscate them in 2008. A small percentage (Gartner estimates less than 10%) of enterprises deploy zero-day signatures, and they do not represent a major competitive factor. The creation of custom signatures by end users is on the increase, although it is in place in less than 20% of deployments, mostly for custom applications or unusual protocols. If IPS vendors provide capabilities for easy offline testing of signatures or filters effective in detecting and/or blocking targeted attacks, then early adopter (Type A) enterprises would increase their use of these features.

IPS products are starting to incorporate features from other emerging security products. Early IPS product offerings include post-connect network access control (NAC) enforcement and data loss prevention (DLP). DLP is not a good fit for in-line blocking, because most DLP concerns are in e-mail and outgoing Web traffic, and effective DLP requires a tight connection to business-specific policies to reduce false positives. However, IPS products can provide simple features for detecting specific types of information (such as credit card and social security numbers) that may offer stopgap capabilities for organizations that are not yet able to deploy DLP (see "Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, 2Q07").

Encrypted traffic is increasing gradually, a significant problem for IPS. As the percentage of Secure Sockets Layer (SSL) and otherwise encrypted traffic increases, it presents a growing "blind spot" when SSL decryption is not in the



product. A small proportion of IPS placement points are less subject to encrypted-traffic problems (for example, behind the analog-to-digital conversion or Web server); however, for most deployments, these difficulties are a growing concern. IPS vendors must include SSL inspection or similar capabilities to meet this challenge.

802.1AE/AF-based networks (see "Q&A on Cisco's TrustSec") will support policy-based link encryption that can decrypt traffic on links where IPS devices are located.

IPS pricing has destabilized significantly during the past 12 months. In 2006, there was a consistent average of \$50,000 per gigabits per second (Gbps) of deep inspection. In 2007, there was considerable price variance. This change is attributed to new IPS features in some products (such as adding vulnerability management integration), making direct product price comparisons less possible, and to some vendors considerably increasing their prices without much change in their products. Thus, enterprises should weight price as a factor in product selections.

Performance, reliability and availability are key criteria for any in-line device. Most vendors include in their base pricing bypass unit modules enabling fail-open for copper ports. Several IPS products are advertised as having speeds of 10 Gbps, although none has any recognized third-party testing to support this claim. Sales of appliances with speeds of 5 Gbps and greater are still rare and often price-prohibitive, with many multi-Gbps placements served with load-balancing several IPSs rather than with one large appliance. As data center and switch IPS placements increase, so will the requirement for these higher-speed devices. Administrative console quality remains a competitive factor. This variance shows mostly in the managing, provisioning and correlating of data from large numbers of devices.