

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are evolving to deliver protection against sophisticated threats, says **Michael Lipinski**.

I think I installed my first IDS back in 2000 and first IPS in 2002. Back then, we had software- or appliance-based offerings, and we chose to install them either in front or just behind our firewalls for an added level of security. The technologies back then were a bit challenging to deploy and did

not offer a wide array of options. As these technologies morphed into stateful firewalls and unified threat management (UTM)-style products, the traditional intrusion detection/intrusion prevention systems have continued to provide a valuable service in our layered defense/security architectures.

These technologies have evolved to support enterprise-wide deployment models. So instead of focusing our intrusion technologies strictly at the gateway traffic, we now have technologies that allow us to gather and manage information as it moves around our networks and to mitigate risks wherever they are found.

IPS 5500 EC/ES-Series



Vendor Top Layer Security
Price \$12,495
Contact www.TopLayer.com

The IPS 5500 Appliance from Top Layer Security is a stand-alone, purpose-built IPS. The EC-Series models have copper network interfaces and built-in zero power bypass functions. The Model 75EC, considered for this Group Test review, is optimized for cost-effective, remote-site deployments.

Typically installed inline, IPS 5500 units can be deployed in a variety of modes, including detection-only, pre-emptive blocking or a combination of both. The Top Layer IPS detection/protection capabilities use integrated three-dimensional protection to perform thousands of inspections to filter out malicious traffic. The solution consists of three main modules: a stateful analysis firewall providing

network-level protection, a denial-of-service protection engine and a deep packet inspection engine providing protection against vulnerabilities, worms and application-level attacks.

The IPS unit is managed through a Java-enabled web browser or through the IPS controller management software. The user interface is attractive with tree-based navigation of configuration and management items and a full graphical dashboard.

Enterprise features for redundancy, failover and scalability are all available. Reporting is granular and based on templates that allow admins to create type and frequency of reports. PCI compliance-level reporting is also available. Event logging configuration is very granular and gives one the flexibility to log as little or as much information as required for each sensor.

The documentation resources are very good, complete and nicely laid

out, making deployment and management of the solution very easy.


The list price includes a three-year threat update subscription, three-year support, maintenance and upgrades, three-year advance hardware replacement, and two-day remote installation and deployment service. Additional support options are available for a fee.



Lot of value for the money. Makes IDS/IPS easy to deploy, use and manage. This solid product gets our Best Buy this month.

Michael Lipinski

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★
Strengths Ease of use, support included for three years, nice integrated offering.	
Weaknesses None that we found.	
Verdict Lot of value for the money. Makes IDS/IPS easy to deploy, use and manage. This solid product gets our Best Buy this month.	



Top Layer Security
 1 Cabot Road, Hudson, MA 01749
www.TopLayer.com • info@toplayer.com
 Phone: +1.978.212.1500 • Fax: +1.978.212.1600