

Catching malware and hackers means you need to know what's going on and act on that knowledge. Christopher Moody gets his hands dirty with a range of IPSs.

The exact definition of an intrusion prevention system (IPS) is a difficult one. A firewall with integrated IDS is one example, a Layer-7 switch another.

In this test we have 12 IPS appliances, covering a wide range of different approaches. We have

applicator-layer switches, dedicated IPS appliances and firewalls with IPS, so there is something on offer for all kinds of networks.

We looked at the number of ports and how they can be configured, examined how fast it can capture data and paid particular

attention to the range of detection methods. Finally, we looked at the range of modes for dealing with a detected threat including, for most events, blocking it immediately.

The type and size of network is likely to be a defining choice when choosing an IPS.

## Attack Mitigator IPS 5500



**Supplier** Top Layer Networks

**Price** from \$15,000

**Contact** [www.TopLayer.com](http://www.TopLayer.com)

This is a 2U chassis designed to block attacks before they cause damage. It sits between the WAN and firewall, rather than inside the firewall as with other products.

With a throughput of 4.4Gbps, it is the top of the range product. But it works at switching speed, so won't put any extra lag on your network.

The basic configuration comes with eight Fast Ethernet, four GBIC and two fixed 1000base-sx ports. The latter ports are used for the High Availability mode with another IPS 5500. The device's availability is further ensured by its dual hot-swap power supplies.

Initial installation is performed through the console port. The set

up guide is easy to follow, and you are soon connected to the Mitigator's Java management console.

It's very easy to use and has a wealth of online information. Set up wizards help you get running quickly and make the initial configuration steps less mundane.

The system works much like a regular firewall complete with a policy. A policy is made up of other objects, such as network ranges and applications, which you can define separately.

The IPS 5500 offers several levels of protection. First, it can recognize harmful viruses, Trojans and exploits, blocking them at wire speed before they cause harm. Second, it can monitor rate-based attacks, such as DDoS and filter the damaging traffic. Finally, it offers access control to prevent unauthorized network access.

It can also create a baseline

reading of the network to work out what's normal and then flag up any anomalies, helping you to stop zero-day attacks. However, the attack signature database isn't as comprehensive as it might be.

If this sounds like a lot to contend with, Top Layer's efficient user interface makes it very easy to deal with even complex tasks.

This is an excellent product. Its wire-speed filtering, first-class management and wide range of tools means it can help secure any network without slowing it down.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★★
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>For</b> Wire speed detection and blocking; SecureCommand gives enterprise-class management.	
<b>Against</b> Small attack signature database compared to other products.	
<b>Verdict</b> Its wire speed blocking and excellent DDoS protection provides top-class security, but it is best used in conjunction with other security products.	



## Reprints

Our Recommended product from the 12 tested is Top Layer's Attack Mitigator IPS 5500. The name says it all - it deflects and blocks attacks before they hit your network. It works at wire speed and is particularly effective at blocking DDoS attacks, arguably the most prevalent kind of attack that networks face today.

Christopher Moody

**Top Layer**

perfecting the art of network security

[www.TopLayer.com](http://www.TopLayer.com)  
508-870-1300  
[info@TopLayer.com](mailto:info@TopLayer.com)  
2400 Computer Drive  
Westboro, MA 01581