

There are fewer real IDS/IPS products in the market as functionality continues to move toward UTM, but there are still some good products, says Peter Stephenson.

This year there are two noticeable changes in IDS/IPS products. First, the footprint we are seeing is decidedly distributed. Second, the functionality continues to approach universal threat management.

There is another trend that, really, is an outgrowth of the function-

ality trend. There are fewer real IDS/IPS products in the market.

But, there still are very credible IDS/IPS products, and from our perspective, that's a good thing. The use of a distributed IDS/IPS is a step forward for most large enterprises. To date there have been ways to gather data from

multiple sensors, but the emerging architecture of separating the control center from the sensors is a step forward.

The products are becoming more versatile, more powerful as analysis tools, and more distributed. And that's good news, indeed.

NitroGuard IPS



Vendor	NitroSecurity Inc.
Price	\$10,495 (Enterprise Security Manager device adds \$19,995)
Contact	www.nitrosecurity.com

The NitroGuard IPS is part of the NitroView suite of products available from NitroSecurity. It is one of a handful of IPS products that allows

detailed analysis of captured events. When used with the rest of the suite, it has extensive analysis capability beyond that normally found in an IPS. The IPS's near real-time dashboard updates as new alerts arrive, rather than using a refresh cycle that does batch updating. We saw this in only one other product.

The product is easy to install and comes with a small installation guide that, though small, provides a good level of detail in such things as physical installation, cabling and selection of an appro-

priate IPS architecture. One manages the appliance remotely from a software console that comes with it and there is an installation guide for the console. If the organization has the rest of the NitroView suite installed, the same console can be used for all obviating separate console installations.

We installed the IPS with the rest of the suite — NitroView Receiver and NitroView Enterprise Security Manager (ESM) — easily and tested with our Attack Pod. The results were excellent with the product identifying our attacks at all levels and delivering its results to the ESM for analysis in near real time. Set-up and rule generation is straightforward and the use of wizards and menus eases the process.

Documentation is complete and comes on a separate CD. The main documentation includes all of the pieces of the NitroView suite so interconnection and interoperability is clearly presented in a single document. The PDF file is well indexed and the information we needed was very easy to find. Keyword/phrase searches, of course, are standard in PDF files.

Support offerings are rich with a

variety of options. For all users there are two sections of the website with such things as manuals and white papers. All one needs to do is sign up. In addition there are extra cost silver and gold support packages with a huge assortment of services, including advance hardware replacement and two-hour response (gold).

Priced at \$10,495, the NitroGuard is at the low end of the range. The ESM offers an enhanced level of analysis and adds \$19,995.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★
Strengths	A solid product with lots of features, including near real-time dashboard refresh.
Weaknesses	None that we could find.
Verdict	A solid product with good integration to other NitroView products, though a bit high priced in its full configuration with the ESM. For its excellent performance, ease of use and flexibility we award NitroView IPS our Recommended rating.



A solid product with lots of features, including near real-time dashboard refresh.

Peter Stephenson



NitroSecurity, Inc.
 230 Commerce Way, Suite 325
 Portsmouth, NH 03801
www.nitrosecurity.com
 800.795.IPS1