

# True network threat analysis goes beyond SIEM

Last month we looked at the Mu 4000, a truly impressive vulnerability analysis tool. At the time I wished that there was a comparable network-based threat analysis tool of the same quality and depth.

And now there is. The latest release of the NitroView Receiver and Enterprise Security Manager (ESM) from Nitro Security is just the ticket if you want to understand your network's response to threats fully and deeply in near real time.

I have been watching Nitro Security for quite some time because their innovative real-time database back-end is beyond anything in the industry in terms of performance and manageability. This back-end has been used in a variety of difficult applications, including intrusion detection, which may be the most challenging. Now that database system forms the basis for the NitroView products and that product suite is as hot as a Fourth of July firecracker.

Forget simple SIM/SEM products or traditional log correlators. NitroView blows them all away in three areas: comprehensive log management, response speed and analysis depth. The suite consists of two boxes (and a potential third if you want to add the NitroGuard IPS reviewed last month). The Receiver is a distributed collector for logging information from just about any source you can imagine. And, if your source does not happen to be supported, talk to Nitro. There's a good chance they can get you the support you need.

## Efficient transfer

The Receiver can be anywhere as long as it can move its data to the ESM for analysis. The Receiver can take data as fast as you can feed it. It really can drink from the high speed network fire hose. It then packages the data for secure, efficient transfer to the ESM. The ESM also can take data as fast as you can get it there. The ESM then analyzes the data and presents it in a variety of ways that answer just about any question you might

come up with relating to the threats against your enterprise.

The ESM is an analyst's dream — from the overall views to detailed drill-down to the individual log entry level. Not only can it take data in near real time, you can feed it collections of logs in bulk and it will happily analyze them (I'm a purist, by the way. I view near real time the way most people view real time. However, if there is any delay at all, no matter how tiny, it is near real time to me). The ESM also provides near real time statistical calculations for the expression of network and security baseline and trend data, an improvement over earlier versions.

## Improvement over earlier release

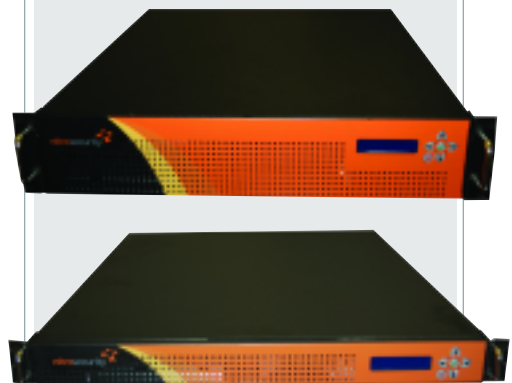
I compared this release of the ESM with the previous one and this product has reached maturity. The improvements over the earlier releases are noticeable from the depth of analysis available to the cleanly reorganized user interface.

As to maintainability, we got a chance to experience this first-hand. During the updating of the database with new data we had three power failures in rapid succession (the test bed is not on a UPS). The database and all its data were fried and we could not restart the box.

This is not normally a problem because in production the data is replicated in at least three places and the system is on a UPS. Since we were just installing, our results were quite different from a production environment. We had to reinstall from scratch and the entire process, from inserting the recovery CD to final configuration and testing, took about 30 minutes and progressed flawlessly. Given that the data would be recoverable easily in production, this normally catastrophic event turns out to be a truly low risk occurrence.

For what you get in these two products the pricing is quite reasonable. I found that it fits nicely with similar classes of products that do not provide as much performance or usability. Support is first rate and I was pleasantly

## AT A GLANCE



**Products** NitroView Receiver 7.2.0 and NitroView Enterprise Security Manager (ESM) 7.2.0

**Company** NitroSecurity, Inc.

**Availability** Now

**Price** Receiver: starting at \$11,995; ESM: starting at \$19,995

**What it does** Provides real-time log management, security event management and network behavior analysis

**What we liked** Speed, depth of analysis, comprehensive log management, enterprise scalability — this suite has it all.

**What we didn't like** Nothing. This is a total network security threat analysis capability in a box (or two, as it happens).

surprised to find that the company's CTO is as much an on-the-road evangelist as he is a CTO in the traditional sense. I like this because it ensures that the engineering and development teams get the users' needs quickly, from a credible source and in language that is meaningful to them.

This is another top-drawer analysis product that we rate as SC Magazine Lab Approved. We look forward to using this tool to benchmark other products in the SC Lab over the next year. Our ability to set up realistic enterprise simulation test beds and monitor their behavior with NitroView will enhance our overall rating test suite. This is another step in making the SC Labs test environment one of the most comprehensive in the industry.

— Peter Stephenson

SC  
MAGAZINE  
Reprints

nitrosecurity



NitroSecurity, Inc.  
230 Commerce Way, Suite 325  
Portsmouth, NH 03801  
www.nitrosecurity.com  
800.795.4771