NIKSUN
Supreme Eagle NetDetectorLive

AT A GLANCE

Product Supreme Eagle® NetDetectorLive™

Company NIKSUN

Price Depends on configuration.

What it does Performs network forensics at carrier line speeds.

What we liked Speed, performance, flexibility and feature-rich. We liked it all.

The bottom line This system really sets the bar for next-generation network forensic analysis tools.

The term "next-generation" gets bandied about a lot these days. Arguably coined by Palo Alto, every marketer trying to differentiate his or her product – and, of course, all do – tags it as next-generation. Sadly for the consumer, most aren't. But every now and again we come upon a real next-generation product. In our cloud security issue [July-August], we found several. And now, in this forensic issue, we have another.

We have been watching NIKSUN for years. The company has consistently produced good products, its thinking is ahead of its time and we made them a member of our Hall of Fame in 2012. That's a pretty strong pedigree. With that said, when a company rep told me about the company's latest product, I was, in spite of their solid history, skeptical. She claimed it was capable of doing everything that the company's current flagship product does and could do it at 100Gbps wire speeds. C'mon, guys, I thought, that's just way too fast for all of the analysis your tools do. But, we are pleased to tell you that we were wrong. And, in fact, we watched it do exactly that. So, for everyone out there working on the next generation of network forensic tools, the fat's in the fire. These guys are setting the bar, and quite high it is, too.

Supreme Eagle NetDetectorLive really is an impressive system. It is configured with parallel processors to make a purpose-built supercomputer that can scale its storage to six petabytes. Functionally, the system can simultaneously capture, analyze and store all network traffic at carrier class line rates and run the data past an IDS, while forensically analyzing captured data and providing notification of detected data breaches and of network anomalies. That is a pretty big mouthful.

We were quite impressed with this system but, of course, it's not for everyone. There are several available configurations and it is priced based on how it is configured. That said, if you have a large mission-critical data stream, you cannot afford not to give this one a close look. When we asked if the system was deployed in the field to real customers analyzing real data, the answer was 'yes,' and the number of customers, given the short time this has been on the street, was impressive.

Deployment, while not trivial, is quite straightforward especially in data centers where administrators are used to complex system configurations. Even here, however, NIKSUN support staff stands ready to help if necessary. If you decide to deploy Supreme Eagle, we suggest that you be clear about your objectives and where you want to collect your data before you start configuration specs.

We predict that every large ISP will want to have one of these, especially given the current threatscape with which they are forced to deal. Recovering from a large-scale network-based attack is not trivial at the best of times, but when the line speeds and amount of data start to climb only the best tools will do. Supreme Eagle NetDetectorLive is one of those tools.

– Peter Stephenson, technology editor

NIKSUN
100 Nassau Park Blvd.
Princeton, NJ 08540, USA
Phone: +1.609.936.9999
Fax: +1.609.419.4260
Email: info@niksun.com