# NIKSUN...Forming the Backbone of U.S. Cyber Protection in the Coming Years

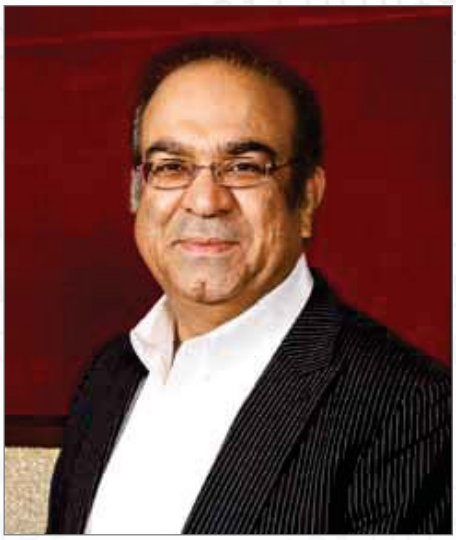
By Jennifer Simoni

In February, you simultaneously announced NIKSUN's Supreme Eagle product, and that you were chosen to be the primary provider of full packet capture capability for the U.S. government's new network protection program, the Joint Regional Security Stacks (JRSS).

## Let's start with the Supreme Eagle product, I understand it's the first of its kind. Can you explain the significance of that for our readers?

We were very excited to announce the public debut of our new product, the NIKSUN Supreme Eagle, because it is an industry-first. With NIKSUN Supreme Eagle, we strive to accomplish the impossible: modular and scalable recording with analysis speeds ranging from 20 Gbps to over 100 Gbps – all on a single hardware platform. It has 15 times more processing capability, requires 60 percent less power consumption, and uses 80 percent less rack space in sharp contrast to any comparable industry solution, which makes it the "next-generation" product, as featured in the October issue of SC Magazine.

While bringing NIKSUN's Supreme Eagle to market is in itself a significant achievement, even more consequential is the fact that we have succeeded where other multi-billion dollar security vendors could not, successfully passed every part of the stringent testing required by the U.S. Defense Information Systems Agency (DISA). With NIKSUN's revolutionary technology, the U.S. Department of Defense (DoD) aims to become a global model in network protection and attack prevention, reemphasizing the importance of cyber security as a key component in the fight to keep our nation safe.



Dr. Parag Pruthi

## And the JRSS, that's a new security division for the US government, can you tell us a little bit more about it and NIKSUN's role in this initiative?

Yes, the Joint Regional Security Stacks (JRSS) is the US government's new network protection program. They stringently evaluated and tested several top vendors for full packet capture, ultimately choosing NIKSUN to provide their full packet capture capability. This is an authoritative testament, not only to the power and uniqueness of our technology, but also substantiates NIKSUN's social responsibility and allows us to achieve our mission in helping keep our nation safe.

As I mentioned in a recent press release on the matter, during times of crisis, the United States and its military, hand-in-hand with an enterprising and innovative private sector, are often called upon to break new ground and set the stage for the future. In this new age of cyber warfare, the JRSS architecture and NIKSUN's revolutionary Supreme Eagle create a pioneering cyber defense architecture that will become the new global standard.

## Back when you started NIKSUN in 1997, cyber threats were very different. What were the biggest challenges your company faced back then?

While the nature of cyber threats was different, they were still as complex given the state-of-the-art in those days. Many people back then believed that antivirus software and a new technology called Intrusion Detection Systems would be sufficient for cyber protection. However, my research showed that science did not back their claims and these "detection" mechanisms were flawed and easily circumvented.

So in the late eighties and early nineties I began to think of a better way. I concluded that with the advent of the network-of-networks, aka the Internet, a revolution was coming where every business and every transaction would move to this open and highly interconnected network as opposed to the closed (leased lines, etc.) networks from a bygone era. At the time, many did not foresee the new applications and services that people would invent to run on top of the Internet. But the Internet would become a new medium for R&D resulting in such a surge of innovation that no single company or institution could keep up with the technology needed to protect its most valuable asset, its intellectual property (IP). But I was confident there had to be a way.

At the same time, my Ph. D. thesis on using chaos to model the erratic, unpredictable behavior of the traffic that traverses the Internet also suggested that statistically speaking the problem was not easily tractable. In a eureka moment, it suddenly came to me that if we could not predict the future, then we could not make the one thing that could "block" the bad stuff out and only let in the "good" stuff into your networks or vice versa keep the "good" stuff from leaking out. And it dawned upon me that if we built a "security camera for the network" then we would have all the visibility we needed, even into unknown incidents and events. Furthermore, if we could take such a security camera and add things like motion detection on top of it, then we could be better at both - recording things that though they may be unknown to us, we could now make them knowable while also alerting on incidents we suspected are bad.

This rationale resulted in the invention of my first two products: NetVCR and NetDetector, which to this day still remain undeniably competitive in the market.

So to get back to your question, the challenges were a) how to record and analyze at wire speeds, and b) how to query the data so you can get answers quickly in fractions of seconds or almost instantaneously. To solve these challenges, we had to solve a myriad of hardware and software issues that were, and to this day still remain groundbreaking.

Well, and all this costs money, so we had to overcome that obstacle as well!

## How has your company and team evolved since then?

With the dissemination of information on a global scale, people began recognizing the real need to secure this data, and yet there was a dearth of effective information security solutions. During this time, we realized that our products, which can monitor and capture everything on the network, and then alert the user if a problem or incident was detected, were perfect for detecting and monitoring security breaches as well. And we weren't alone in this realization.

In 2004-2005, the United States Secret Service (USSS) was overwhelmed by an international group of cyber criminals who had created a stir in the banking fraternity by hacking into databases and stealing close to 1.7 million credit card numbers. Millions of dollars were lost and this cyber attack was estimated to cost us close to billions of dollars. W. Ralph Basham, the Director of the USSS at the time (2003-2006), got word of a company that was engaging in network monitoring solutions to secure critical infrastructure. After a meeting behind closed doors, I was entrusted with building a solution to tackle these infringements. My team and I were able to design and deliver a product to the USSS with the technology to lawfully intercept and analyze large amounts of data streaming through networks.

This is just one example. We have and continue to help many corporations, both big and small, not only resolve cyber incidents, but also keep monitoring their network infrastructure so that they are able to take effective measures against those attempting to break into their systems.

To give you an idea of the scope of some of our deployments – for one customer we are analyzing over 3 Tbps of traffic for over 20 Petabytes, every few hours, for instant incident response. In order to cater to such high demand for our products and satisfy the growing number of customers, we have had to build a terrific team. We selectively hire the very best engineers to support our back office operations, in fact in every part of our business. It is not easy finding, training, and retaining such talent. But we have done it now for almost two decades.

This is how NIKSUN has evolved over the years – creating state-of-the-art technology that has proven its chops time and time again. It is a powerful force called into many delicate matters.

## You supply services to governments, agencies, enterprises, retailers, manufacturers. What are some of the common challenges these institutions face when it comes to security? (or conversely, is there something unique you see with one group over the others?)

While all of these groups care about cyber security, they do so for completely different reasons. Governments for example, they are in the business of protecting the nation's valuable data from other countries – it is a matter of national security. Retailers, on the other hand, care about protecting their customers' data because for them, a security breach (think TJX or Target), may result in tremendous financial loss as well as customer attrition. Customers might not feel safe in providing these retailers with their credit card information; thus, the retailer takes a double hit, both financially as well as a tarnished reputation.

So even though different groups care about cyber security for different reasons, it all comes down to the same variable – protecting data.

Unfortunately the cost to these institutions once they have a breach is very high. What NIKSUN does is that it helps prevent such breaches in the first place and if a breach should occur, due to automation of our solutions, the cost of detection and mitigation is really minimal when compared to the financial losses incurred. These losses could exponentially grow from tens to hundreds of millions of dollars, very quickly. In a nutshell we have saved our clients hundreds of millions of dollars.

## What brings a company to NIKSUN for the first time? Is it prevention or is it because of a known problem?

It is both – a known problem, and prevention. Unfortunately, many times customers come to NIKSUN after they have suffered a cyber attack. They suddenly realize that they need to pay attention to securing their network, and with our extensive product line, we are the logical choice for them.

Others have security teams in place that already know the cost and devastation of a security breach and proactively seek out NIKSUN, for security detection and prevention. We have been around for almost twenty years, consistently perfecting our technology, and our customers trust us.

## What one bit of advice would you give our readers about enterprise security?

My one bit of advice regarding enterprise security is: be proactive not reactive. Get busy securing your network now, so that you aren't the next victim of a cyber crime. It is not a matter of if, it is really a matter of when. Don't make security an afterthought – it could cost you millions. And if you do have enterprise network security in place already, ensure you are using a solid vendor, who not only has a proven track record but has also been endorsed by government agencies, ISPs, large enterprises, as well as financial institutions. These endorsements provide the unequivocal truth that your security solution is worth its salt. ■