



## IT security must innovate or die, NetEvents conference told

12 February 2011

Luke Collins



Network security companies must innovate or die, according to Nir Zuk, founder of next-generation firewall company Palo Alto Networks.

"Innovate or die – Those are the two options that every high-tech company in the world faces," Zuk told delegates at the NetEvents conference in Barcelona last week.

Speaking two days before Friday's announcement of a tie-up between Nokia and Microsoft, Zuk got little response when he asked the audience how many of them had a Nokia smartphone, or used Microsoft for search.

"What happened? Nokia did not innovate, and they let other companies innovate and run them over. They're dead. I just don't how they're going to survive this smartphone war.

"What happened to Microsoft? Look at Microsoft versus Apple – they just stopped innovating. They thought that they controlled the world, that the entire world was in their hands and that everyone would continue using Microsoft software forever, and in the meanwhile others came from behind and passed them."

Zuk argues that the same is happening in the hardware firewalls business, where he claimed innovation is stagnating.

"The technology that enterprises use to protect their networks today? All that technology was designed around 1995. Nothing has changed since I built the first firewall at Checkpoint Security."

Zuk argued that threats to corporate security have evolved rapidly, with 96 per cent of corporate network users using web-based file sharing, and applications such as Salesforce.com, WebEx and Sharepoint all offering new vulnerabilities. The dilemma for security professionals, Zuk said, is that "you can't allow applications such as LinkedIn because there's a lot of risk associated with them, but you can't block them because the enterprise needs them."

Zuk said the \$10bn a year that companies spend on protecting web and email traffic is like the building of the Maginot Line in France - the threats just route around it.

"The traditional response [to the threat of these web-based services] is to block the applications and the users - but that is not innovation. That is going backwards.

"What companies do is to get the IT department to say no to everything. But it is IT's role to enable the business. What you need to do is to extend security to all these applications. If you scan web traffic for viruses, you should do the same for WebEx traffic."

Palo Alto Networks is building what it calls 'next-generation' firewalls that don't classify traffic on the basis of the port it arrives on and the protocol it uses, but on the basis of what the application is, who the user is, and what the user is trying to do with the application.

Bob Walder, research director for security, privacy, and risk, infrastructure protection, at Gartner, said that other firewalls and security devices were becoming more aware of applications.

Zuk countered: "They're not getting the point of application awareness. They think it is about blocking Facebook. It's not about controlling the application - it is about securing the application."

<http://eandt.theiet.org/news/2011/feb/innode.cfm>