# Stanford eCorner

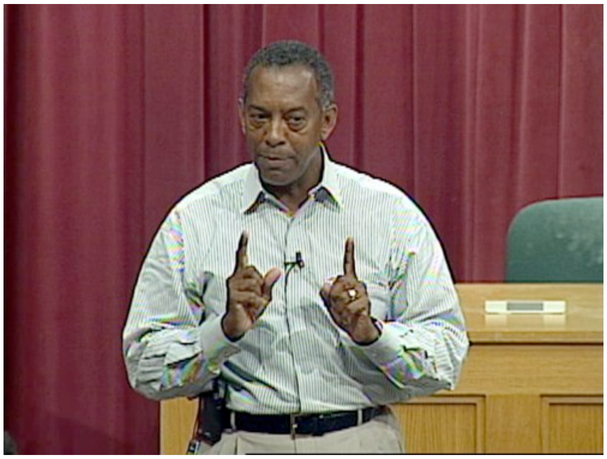
## Identifying Opportunities: Intrusion Detection

**John Thompson, *Symantec Corporation***

**May 23, 2003**

**Video URL:** http://ecorner.stanford.edu/videos/355/Identifying-Opportunities-Intrusion-Detection

Intrusion detection is the next big opportunity, says Thompson. However, it is 10% the size of the antivirus market, and is therefore relatively small. First generation intrusion detection technology was very difficult to deploy and manage he notes. Now these customers, especially those in the financial space, want intrusion prevention technology. Migration from software to hardware is first driven by desire to improve line speed. Thompson talks about ways in which many companies are adopting this model. Symantec chose an alternate model because it is primarily a software company.



### Transcript

Intrusion detection is the next big opportunity, I think, in the security space but let's put it in context. It is 10% the size of the antivirus market so arguably, it's relatively small. It'll be $300 million or $400 million now. That's not chump change but that same antivirus market is $3.5 billion. So while we play in the intrusion detection market, our core business is 10 times the size and growing faster interestingly enough than the intrusion detection market is right now. Why is that? First generation intrusion detection technologies were very, very difficult to deploy. More importantly, very difficult to manage once they were deployed. So many customers, primarily in the financial services sector that deployed early-stage first generation intrusion detection found the promise a bit hollow and hence, as they looked at second generation intrusion detection they want to move more toward the prevention model which is don't detect that something's there and then tell me something's knocking at your door. Stop it from coming into my house and hence, intrusion prevention is focused very much that way. The migration from software to hardware is first driven by the desire to improve line speed, improve the performance of the sensor.

Many of the early-stage first generation software sensors could barely reach 150 to 200, maybe in some instances 300 megabits. Massive networks perform at multi-gigabit speed. The firewalls perform in that speed so if you're going to have an intrusion sensor, it needs to perform at gigabit plus speeds as well. So one of the ways in which you take first generation software and give it gigabit performance is you wire it down, if you will, to a specific ASICs-based hardware appliance and that's what some companies have done. We chose a different approach. Our approach was by the fastest software product we can buy and then find over time the right hardware platform to nest it on. So the manhunt product runs at just shy of two gigabit as a pure play software product on a Dell or a Compaq or an HP PC. If we chose to wire it down to an ASIC, you can imagine that it would run substantially faster than that, but we're a software company; we're not a hardware company. While we do some dibble-dabbling with security appliances, I call it dibble-dabbling because it's a small amount of revenue I'd like for it to be. Dibble-dabbling, a lot of revenue, but right now it's not.