

## Savvy Companies Focus First on Security Goals

*IT Business Edge*  
December 14, 2007

By Carl Weinschenk

*With Seth Birnbaum, CEO of [Verdasys](#).*

**Question:** Can you describe the shift in the security market?

**Birnbaum:** There has been a dislocation in the security market. There is a massive shift in IT and infrastructure security. It's no longer a big deal about the perimeter. The point product infrastructural approach, the layer-by-layer approach, won't scale and is too complex for companies to use for the actual protection of data. The other profound shift is that security is not something IT guys alone need to worry about. We are selling to business units. CEOs, CFO and boards are tasked with the question of what the company is doing to protect data and customers. It's really an opportunity for leadership.

**Question:** What is the new dynamic?

**Birnbaum:** What it boils down to is a set of use cases. A customer example: When we started at (insurer) Humana, they were looking at a product, their particular use case was an algorithm on a Humana laptop. They wanted the laptop to know that when it was in the office, customer data can flow to the network, to the printer and elsewhere. When the machine was at a Starbucks, they wanted the computer to be aware it was no longer on the network, so don't let anything flow except back through a VPN to the corporate network. It is almost like data vaulting based on what kind of connection there is. That was about two years ago. That was the initial use case. We rolled that out to 36,000 users. Someone at Humana then said that they were worried about USB-connected cards, CDs and other portable media. So we started looking at products and rolled out Digital Guardian to all their devices.

**Question:** So how significant is the change from a focus on point products to an emphasis on how the data is used, stored and transported?

**Birnbaum:** It's a huge shift. Perhaps the most profound part is that customers want sets of use cases, they are going away from the point solutions that don't address the use cases. The shift is profound at the purchasing level, the way they are thinking about purchases. It is different than what the Symantecs and McAfees are providing through their channels. DLP [data loss protection] is addressed in 20 percent of the use cases. It's a progenitor, a leading indicator of the data security market.

**Question:** How many use cases are there?

**Birnbaum:** I think it's cooking down to a general set of 20 to 30 use cases. The real power of what we are doing is that we can deliver it all from a single system. Another example would be automated encryption of sensitive data. Another is assured deletion — making sure I deleted something — and another is auditing of data level transactions. Some companies ultimately use the technology for all their security, but don't deploy on the same date. That's how the new data security model works. Each new use case works [and does something additional].

**Question:** What does Verdasys build?

**Birnbaum:** We create data monitoring, data flow control, adoptive encryption. Our policy [engine] controls all the data of the company in a way that is very scalable. We have both context- and content-based classifications and impose rules around how the data is going to be used.

**Question:** Will other vendors have to shift their approach as well?

**Birnbaum:** Vendors have to have a deep and direct technical relationship with the customer. That means spending a lot of time with customers. The people spending time at those companies need to be technically sophisticated. At Verdasys, all salesmen have engineering training. The use case approach requires a sophisticated understanding of customers' problems and issues. We also invest in training about what is in the field, both our technology and what the others do. Investment of engineering as a percentage of company spending is increasing as well.

**Question:** Do companies "get it?"

**Birnbaum:** Yes, once they see one system. I think universally across companies there is a more mature dialogue on information risk management. Whether they communicate better or not I am not sure, but the dialogue about data risk is more mature. There is a sense in the market that the old strategy is not working anymore. There is enormous growth. The market for data security as distinguished from IT security is huge.

**Question:** Will the cost-per-sale be higher?

**Birnbaum:** The cost of doing business is much higher in the absolute sense because it involves six or seven different point products. Ultimately the cost point for the customer is better. The real challenge is integrating it into a solution for customers that works. There are a lot of baskets of point products that are not integrated and can't ultimately fulfill the use case. There have been a number over the years. These generally are called Frankenstein products, because Frankenstein moved in a herky-jerky way.

**Question:** Where does network access control fit in?

**Birnbaum:** NAC is great for managing machines. It's not great for managing data. The adoption cycle is slow. Our customers demand data-level access control. We have a lightweight client to complement NAC. It is a piece of software in front of the server or application. It is used to access data — it is not meant to replace the NAC. It's very complementary and provides protection for the data. NAC in and of itself doesn't get you home.