



[Back to article](#)  [Print this](#)

Data leakage prevention becomes a feature

Along with anti-spyware apps, spam filters, IDSes, and firewalls, DLP may go from stand-alone platform to become regular part of bigger packaged security suites

By Matt Hines

November 26, 2007

Driven by market consolidation and the ongoing efforts of large IT security vendors to meld DLP (data leakage prevention) tools into their broader portfolios, some experts contend that the technologies will increasingly become perceived as product features and less so as stand-alone platforms.

As with countless other security technologies that previously flourished as separate products but are now largely consumed as elements of packaged security suites -- including anti-spyware applications, spam-filtering tools, intrusion detection systems (IDS), and firewalls -- some market watchers claim that DLP is rapidly shifting into a mere piece of other offerings.

Over the last six months, a slew of independent DLP vendors have been acquired by large security providers, including Vontu, Tablus, Provilla, PortAuthority, and Oakley Networks.

Just as customer demand for DLP technologies -- considered valuable tools in stemming the theft and misplacement of sensitive corporate information -- drove Symantec, EMC, Trend Micro, WebSense, and Raytheon to buy those firms, respectively, the ubiquitous need for data protection among enterprises will drive further integration of the applications into other systems, according to some industry watchers.

"If you look at what DLP does, the real value will become more of a stack value than a vertical play," said Jon Oltsik, analyst with Enterprise Strategy Group. "A lot of devices can do packet filtering at the edge, and that filtering will become the enforcement of a policy, versus stand-alone data leakage prevention; the DLP system will still be where you might classify data, enter policies, and do analysis, but other products will likely take over the enforcement piece."

As Symantec had not yet announced details of its [\\$350 million deal to buy Vontu](#) when the market leader convened its second quarter earnings call on Oct. 23, Chief Executive John Thompson deferred questions about the impending acquisition in favor of highlighting DLP features that already resided in a number of the company's existing products, such as its database security programs.

While Symantec executives claim that the firm is planning to continue to sell Vontu's technology as a stand-alone platform for the foreseeable future, they also concede that one of the major benefits of adding the startup will be giant vendor's ability to further weave the acquired tools throughout a number of its other products.

"If you're going to have an agent on the end point, clearly you want all those capabilities to be integrated, and that includes DLP," said Ken Schneider, chief technology officer of Symantec's Security and Data Management group. "One of the things we're always trying to do is take disparate sets of technologies and build them into our architecture; we will continue to sell DLP as a stand-alone, but we will also introduce DLP capabilities throughout the portfolio."

As with many other security technologies, one of the hardest parts of effectively using DLP tools in the enterprise setting lies in customers' abilities to manage the systems, Schneider said.

Based on that reality, the degree to which Symantec can bond the technology with other security tools to allow for centralized management and policy control will play heavily into further adoption of DLP applications, according to the executive.

At rival McAfee, which has made less aggressive moves in adding DLP capabilities -- [having purchased a smaller vendor, Onigma](#), in late 2006 and [recently buying Safeboot](#), more of a device encryption specialist -- executives agreed that the complex nature of the data protection tools makes integration crucial to their overall usability.

McAfee executives agree with Symantec's view that there is likely a market for both stand-alone and integrated DLP in the short term, but said that the long-term play favors assimilation into other products -- in particular, more narrow DLP products aimed at protecting only end points, network gateways, or databases will need to be merged with other technologies, said Vimal Solanki, McAfee's senior director of product marketing.

Those DLP products that can offer broader coverage across different systems and many types of data have the best chance of selling on their own going forward, he said.

"The point products that are out there are just features at some point, if they don't have all the pieces, like encryption, they won't meet all the expectations that customers have for DLP," Solanki said. "The key is that the same policies have to apply regardless of the device or the data; vendors have done a good job of marketing individual DLP features, but what we've seen among customers is that unless they can view many areas of risk and manage them with the same policy, DLP becomes a much tougher sell."

Some companies who have already been acquired are already questioning the viability of the DLP space they came from.

"The remaining stand-alones will be very challenged, as DLP is going to be absorbed into all types of networking gear," said Derek Smith, chief executive of Oakley Networks, which was acquired by defense industry giant Raytheon for an undisclosed sum in late September. "I think DLP was probably pretty short-lived as the basis for an entire company, because if all you are doing is putting a box on the network, you're simply deflecting the threat of data loss to another vector that you probably can't see."

However, most people in charge of the 35-odd remaining independent providers of DLP tools argue that in many senses it is the larger vendors who have the most work to do.

It is the core anti-virus tools and spam-filtering products of security companies including McAfee, Symantec, and Trend that are becoming rapidly commoditized, an argument that has hung over the sector for years, said Seth Birnbaum, chief executive of Verdasys, an independent DLP vendor.

The big players are trying desperately to shift from selling those types of legacy products into providing the data protection tools that customers are clamoring for, he said.

"Maybe if we were more of a point provider I'd be worried, but we are winning deals today based on a platform approach that includes everything from data discovery and policy creation right through to encryption, which is what customers are looking for and not many people have been able to offer," said Birnbaum.

"These bigger players are going to have a much tougher time trying to realign their entire business around data security since they've been married to all these other product lines for so long," he said. "The stronger point providers will be acquired, and everyone who doesn't have all the necessary pieces of DLP will be wiped out, but there's a lot of room for those of us who are already doing it the right way today."

Other stand-alone vendors admitted that there is probably value to be found in arguments for both independent and integrated DLP systems.

"The answer is that we will probably see escalation of both models," said David Etue, vice president of product management at Fidelis Security, another independent DLP vendor.

"Some of early DLP market success stories were people were who built more of a feature, and I'm not sure if it was their strategy, but they built something that easily became a feature of other things," he said. "At the same time, we obviously believe that those of us who sell a real DLP platform today continue to have a strong opportunity."

Other analysts contend that the stand-alone DLP market does in fact have sustainability but claim that there will only be a few players-- those who have mastered the policy management and enforcement pieces specifically -- who will survive and potentially flourish.

At this point, any company whose products do not offer that level of functionality are probably living on borrowed time, said Rich Mogull, a longtime analyst at Gartner who recently launched his own consulting firm, Securosis.

In the case of the larger vendors such as Symantec, the analyst said that the company will integrate its DLP tools with other products, while also marketing the policy management and enforcement aspect of the technology as a stand-alone product.

"There are a lot of elements of content monitoring and protection that can be integrated on the firewall, the end point, or in e-mail, and those more narrow providers who address only those things will probably go away," Mogull said. "For Symantec to connect Vontu's DLP to its end-point products makes sense, but there's still a market for the technologies used to create, manage, and enforce the policy, something for all these other systems to plug back into."

"The independent companies who already have a platform and can address the high-level business problems of protecting data will likely be the ones who get acquired next," he said. "But there's probably only a dozen or so left like that, because many of the companies that have identified themselves as DLP only solve a small part of the problem."

 [Print this](#)