

Product focus evolves in volatile data loss prevention market

By Neil Roiter, senior technical editor, *Information Security* magazine
29 Nov 2007 | SearchSecurity.com

If you think of data loss prevention (DLP) as simply some sort of information firewall to protect credit card numbers from careless employees or criminals, think again. We're increasingly unable to manage and understand the many ways and places in which our data is created, replicated, moved and shared--much less protected.

"Our whole approach relies on the norms of IT of the previous decade--a closed network world in which you control who has access, with most of your information of value sitting within traditional applications," said John Meakin, group head of information security for Standard Chartered Bank, a Workshare customer. "With the trends the trends towards outsourcing offshore and Internet intercourse, I believe those norms have broken down."

The young DLP market is consolidating even as the tools are evolving to address this reality. Earlier this month, Symantec finally confirmed information security's worst kept secret, its intention to acquire Vontu, one of the generally acknowledged market leaders, along with Vericept. McAfee entered market when it snapped up Onigma, and EMC expanded its growing security portfolio by acquiring Tablus. Trend Micro (Provilla) and Websense (PortAuthority) have also moved in.

But moved into what?

"We feel very strongly that this is something that will go to desktop; it's related to broader information management," said Jonathan Penn, vice president and research director at Cambridge, Mass.-based Forrester Research Inc. "Once you can understand the data people are working with, especially in context, you can apply it to whole lot of thing besides security, including storage and knowledge management, search and retrieval,"

Penn said EMC is "a great example" to meet companies' needs because of its position in information management, along with Microsoft, Oracle, Symantec and, possibly, Cisco. IBM's plans to spend \$1.5 billion on security research and possible acquisitions in 2008 marks it as a prime player as well.

Savvy corporate IT security executives get this comprehensive view of information management and security. Broadcom, for example, needed to understand how its intellectual property moved throughout the organization so it could protect it without stifling the free flow of information among its research and development staff, who make up 75% of its employees.

"In highly collegiate environment, it's very difficult to define who has access to what because of fluidity and groups changing," said Broadcom CIO Ken Venner, who uses Verdasys Digital Guardian to "follow the flow of info and determine if it is flowing the way you want it to flow."

"We now understand how people were working and how *we thought* they were working--what they were doing, how they were doing it and how they shared info. Every employee and contractor machine has mechanisms for alerts and/or summary reports to show management how intellectual property is flowing."

"You need a mechanism to allow you to see how information passes over you own networks and to others. Traditional information security tools haven't kept up," said Meakin, explaining why Standard Charter uses Workshare. "We can't allow information to spread without making sure the appropriate security questions are answered and appropriate actions taken."

"The question is: Will DLP remain a market in and of itself? Some companies will just have content security, some desktop," said Forrester's Penn. "Symantec will put it into all sorts of products on the database side, IDS, email, archiving and storage management as well."

Nonetheless, independent companies like Workshare and Verdasys are examples of the diversity among the players in the DLP market--and how it is changing. Verdasys' focus has been on the device, where the data is created, tracking and capturing user activity. Workshare started in DRM space but has expanded the scope of its offering significantly. Both have just announced major upgrades.

Verdasys Digital Guardian 5.0 combines context management--taking things like source and destination, user information and file type into consideration--with content inspection. It also features policy-driven file and email encryption and application logging and masking.

Workshare's new Unified Content Protection (UCP) Suite provides central management for endpoint and gateway modules and tools including full disk encryption, USB security, secure PDF, data discovery and fingerprinting.

Most of the early DLP entries focused on inspecting outbound data at the gateway, adding desktop components when it became clear that the perimeter approach was limited and security heavyweights like McAfee broke into the market on the desktop.

"You see cross pollination, folks who traditionally focused on desktop and folks focused on the gateway validating each others markets," said Eric Ouellet, a research vice president at Stamford, Conn.-based Gartner Inc. That is why you are seeing companies like Vontu building up their client for their 8.0 release."

Symantec, which has partnered with Vontu to beef up its email security appliances, expects to integrate Vontu's technology into a number of its own products, while still offering stand-alone DLP.

"It's information-centric security," said Ken Schneider, chief technology officer for Symantec's security and data management group.

Commenting on the \$350 million Symantec is shelling out for Vontu, Schneider called the acquisition "strategic," but believes there's a lot of money to be made in the growing DLP market, which is now somewhere between \$100 million and \$200 million depending on who you talk to.

"In a couple of years, every global enterprise will have DLP, a couple of thousand companies spending hundreds of thousands of dollars each," he said.

"The trend for the next year will be around the "hygiene" vendors (antivirus vendors, for example). but then we'll see a growth market around the data discovery side of things," said Gartner's Ouellet. "EMC and Vontu--which means Symantec as long as they beef up other functionalities--are providing decent data discovery."