

Magic Quadrant for Content-Aware Data Loss Prevention

Gartner RAS Core Research Note G00200788, Paul E. Proctor, Eric Ouellet, 2 June 2010, V2 RA2 12062010

The enterprise content-aware data loss prevention market has gone through a significant shift. Vendor consolidation has slowed, and the market has bifurcated into “high-end” enterprise capabilities and “low-end” channel capabilities offering more choices to organizations of all sizes and needs.

WHAT YOU NEED TO KNOW

Organizations seeking content-aware capabilities to address sensitive data have more options in 2010. The data loss prevention (DLP) market has gone through many changes. These include the continued commoditization of endpoint products, the rise of content-aware functions in many traditional security and infrastructure products, and the integration of identity awareness in traditional DLP products. Market consolidation has slowed, and the larger vendors are making more enterprise deals as DLP matures into a common control within the standard of due care.

A number of other security solutions provide content-aware functions and limited DLP. These include e-mail boundary security, secure Web gateways (SWG) and endpoint protection platforms. In many cases, the limited DLP feature set in these channel-specific solutions (C-DLP) is sufficient to solve near-term business requirements for DLP. Indeed, Gartner projects that the majority of organizations (approximately 70%) may be able to deploy “good enough” DLP capabilities in evolving channel-specific solutions to satisfy government regulations with respect to private and sensitive data, and for the automated application of protection mechanisms such as encryption of e-mail, and the storage of sensitive content to USB and other removable storage media or portable devices.

Purchasing criteria should be based on a good enterprise DLP strategy that addresses the fundamental question: Will channel DLP be sufficient to address your sensitive data requirements or will you need a more comprehensive enterprise DLP product? In 2010, we change our guidance regarding the purchase of endpoint DLP to encourage its adoption at the right price, which is now less than \$30 per seat for a fully functional enterprise DLP endpoint or less than \$15 per seat for a content-aware channel DLP endpoint as part of an endpoint protection platform purchase.

MAGIC QUADRANT

Market Overview

Content-aware DLP tools enable the dynamic application of policy based on the classification of content determined at the time of an operation. Content-aware DLP describes a set of technologies and inspection techniques used to classify information content contained within an object — such as a file, e-mail, packet, application or data store — while at rest (in storage), in use (during an operation) or in transit (across a network); and the ability to dynamically apply

a policy, such as log, report, classify, relocate, tag, encrypt and/or apply enterprise data rights management (EDRM) protections. DLP technologies help organizations to develop, educate and enforce better business practices concerning the handling and transmission of sensitive data.

Used to its full capability, DLP is a nontransparent control, which means it is intentionally visible to an end user with a primary value proposition of changing user behavior. This is very different from transparent controls such as firewalls and antivirus programs that are unseen by end users. Nontransparent controls represent a cultural shift for many organizations, and it's critical to get business involvement in the requirements planning and implementation of DLP controls.

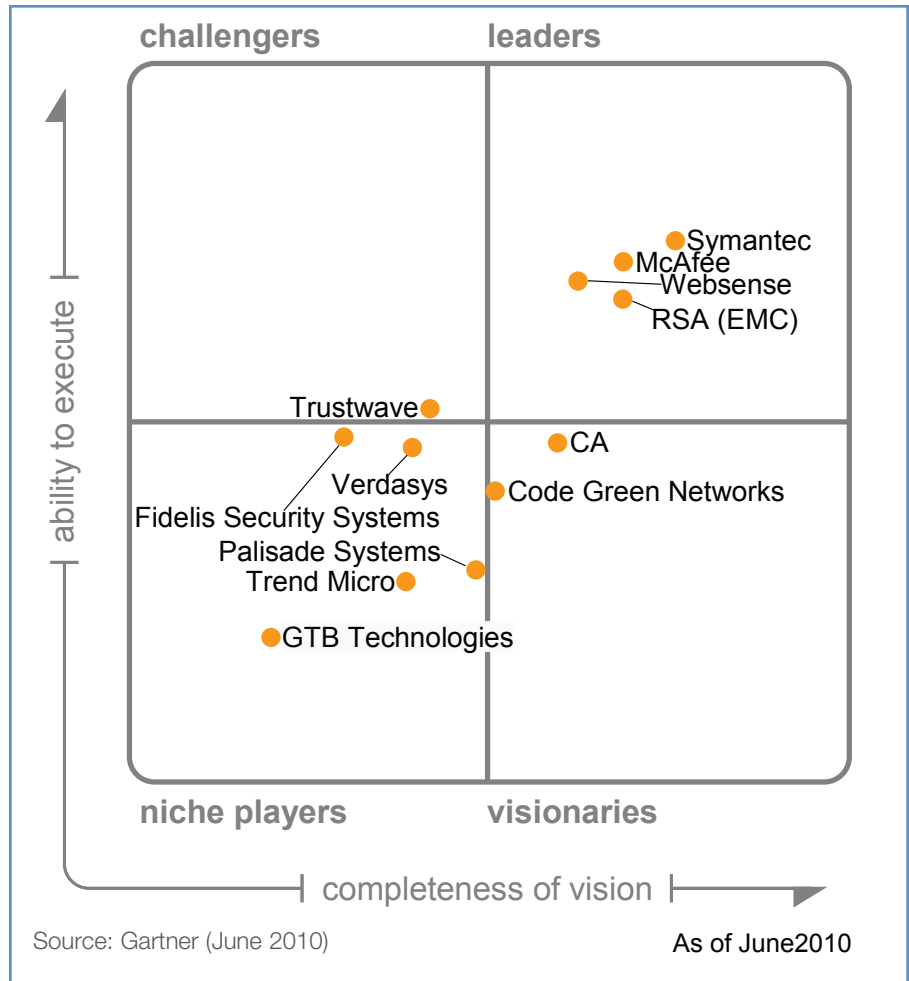
As DLP tools mature, use cases for managing sensitive data are becoming more sophisticated. Use cases associated with social media have become more common, especially those involving operations when the computer is not connected to the corporate network. An example of this would be detecting the posting of sensitive data to social-media sites while sitting in a coffee shop. Features that support these use cases include endpoint, network functions, Web proxy integration and the ability to resolve an IP address with a user name. Support for these features varies widely between the vendors — in some cases requiring custom integration with Microsoft Active Directory or other services.

Many vendors are experimenting with alternative delivery models, such as cloud and software as a service (SaaS), for monitoring some types of network traffic (such as Web and e-mail). Organizations should approach this cautiously and understand that detecting sensitive data in the cloud has data propagation issues that must be addressed, such as notifying third parties of the presence of sensitive data outside the organization's boundaries. Vendors with notable DLP functions available through cloud and SaaS include Symantec, Trustwave and Websense.

Gartner inquiry data through 2009 indicates three major observations that should help organizations develop appropriate requirements and select the right technology for their needs:

- About 40% of enterprises led their content-aware DLP deployments with network requirements; 20% began with discovery requirements; and 40% started with endpoint requirements. Enterprises that began with network or endpoint

Figure 1. Magic Quadrant for Content-Aware Data Loss Prevention



capabilities nearly always deploy data discovery functions next. The majority of large enterprises purchase at least two of the three primary channels (network, endpoint and discovery) in an initial purchase, but few deploy all three simultaneously.

- Many enterprises struggle to define their strategic content-aware DLP needs clearly and comprehensively. We continue to recommend that enterprises postpone investments until they are capable of evaluating vendors' offerings against independently developed, enterprise-specific requirements.
- The primary appeal of endpoint technologies is protecting intellectual property and other valuable enterprise data from insider theft and accidental leakage (full disk encryption mitigates the external theft and compliance issues). The value of network and discovery solutions, by contrast, lies in helping management to identify and correct faulty business processes, identifying and

preventing accidental disclosures of sensitive data, and in providing a mechanism for supporting compliance and audit activities.

The embedding of content-awareness functions in more products will enable the broad, effective application of protection and governance policies across the entire enterprise IT ecosystem, and throughout all the phases of the data life cycle, becoming what Gartner refers to as a content-aware enterprise. Enterprise DLP vendors will support APIs that can manage and exchange common detection policies and response workflows with other components by 2012.

Market Definition/Description

Gartner defines content-aware DLP technologies as those that — as a core function — perform content inspection of data at rest or in motion, and can execute responses, ranging from simple notification to active blocking, based on policy settings. To be considered, products must support sophisticated detection techniques that extend beyond simple keyword matching and regular expressions.

This market has steady growth. Content-aware DLP deployments and overall sales were only minimally affected by the economic downturn. Gartner believes this market will reach \$400 million in 2011.

Inclusion and Exclusion Criteria

Vendors are included in this Magic Quadrant if their offerings:

- Can detect sensitive content in any combination of network traffic, data at rest or endpoint operations
- Can detect sensitive content using sophisticated content-aware detection techniques, including partial and exact document matching, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual and lexicon analysis
- Can support the detection of sensitive data content in structured and unstructured data, using registered or described data definitions
- Can block, at minimum, policy violations that occur via e-mail communication
- Were generally available as of 31 January 2010
- Are deployed in customer production environments, with at least five references

Vendors must also be determined by Gartner to be significant players in the market, because of market presence or technology innovation.

Vendors are excluded from this Magic Quadrant if their offerings:

- Use simple data detection mechanisms (for example, supporting only keyword matching, lexicon, or simple regular expressions)

- Have network-based functions that support fewer than four protocols (for example, e-mail, instant messaging and HTTP)
- Primarily support object tagging and then enforce policy based on the tags

Added

Trustwave

Dropped

Vericept (acquired by Trustwave)

Evaluation Criteria

Ability to Execute

Our ratings are most influenced by three basic categories of capability: network performance, endpoint performance and discovery performance. We also considered the actual level of product integration with internal partners (if content-aware DLP capabilities came through an acquisition) or external partners, as part of the analysis.

Completeness of Vision

Content-aware DLP technologies are becoming more mainstream in North America, Europe and Asia. Many recently acquired providers have seen their offerings transformed into part of an overall platform, taking on greater breadth and depth of capability in the process. The Gartner scoring model favors providers that demonstrate completeness of vision — in terms of strategy for the future — and ability to execute on that vision. Gartner continues to place a stronger emphasis on technologies than on marketing and sales strategies. A clear understanding of the business needs of DLP customers — even those that do not fully recognize those needs themselves — is an essential component of vision. This means that vendors should focus on enterprises' business- and regulation-driven needs to identify, locate and control the sensitive data stored on their networks and passing their boundaries.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	no rating
Sales Execution/Pricing	high
Market Responsiveness and Track Record	standard
Marketing Execution	no rating
Customer Experience	high
Operations	high
Source: Gartner (June 2010)	