

Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention

Gartner RAS Core Research Note G00157450, E. Ouellet, P. Proctor, 17 June 2008, R2775 06182009

The market for CMF and DLP technologies is maturing rapidly and has undergone significant restructuring due to many acquisitions during the past 12 months; however, it remains fundamentally adolescent. Vendors must recognize that addressing business requirements is critical for their success.

WHAT YOU NEED TO KNOW

This document was revised on 18 June 2008. For more information, see the Corrections page on gartner.com.

In 2006 and 2007, the data loss prevention (DLP) market, which Gartner previously called the content monitoring and filtering (CMF)/DLP market, was dominated by vendors offering network-based, content-aware mechanisms typically used to detect sensitive data crossing the enterprise perimeter outbound. In 2008, sophisticated, content-aware functions became more commonly available in a variety of technologies, including end-point protection, network communication analysis, sensitive data discovery, document management and e-mail encryption products. This wide availability of content-aware mechanisms offers benefits and problems for enterprises seeking to deploy DLP. The available choices are increasing, and the overall maturity level of the market is rising, but it is becoming more challenging for enterprises to develop a coherent CMF/DLP strategy. DLP offerings are maturing very quickly, and 2008 road maps will provide significant upgrades if and when they become a 2009 reality.

Enterprises that do not yet have a clear and comprehensive statement/definition of their strategic DLP needs should postpone investment in this technology until 2009. It is critical at this stage of market development that a vendor's offerings be evaluated against a set of independently developed, enterprise-specific requirements. Enterprise customers must not allow vendors' claims – for example, that their templates address all requirements – to lull them into the mistaken belief that all their needs will be met.

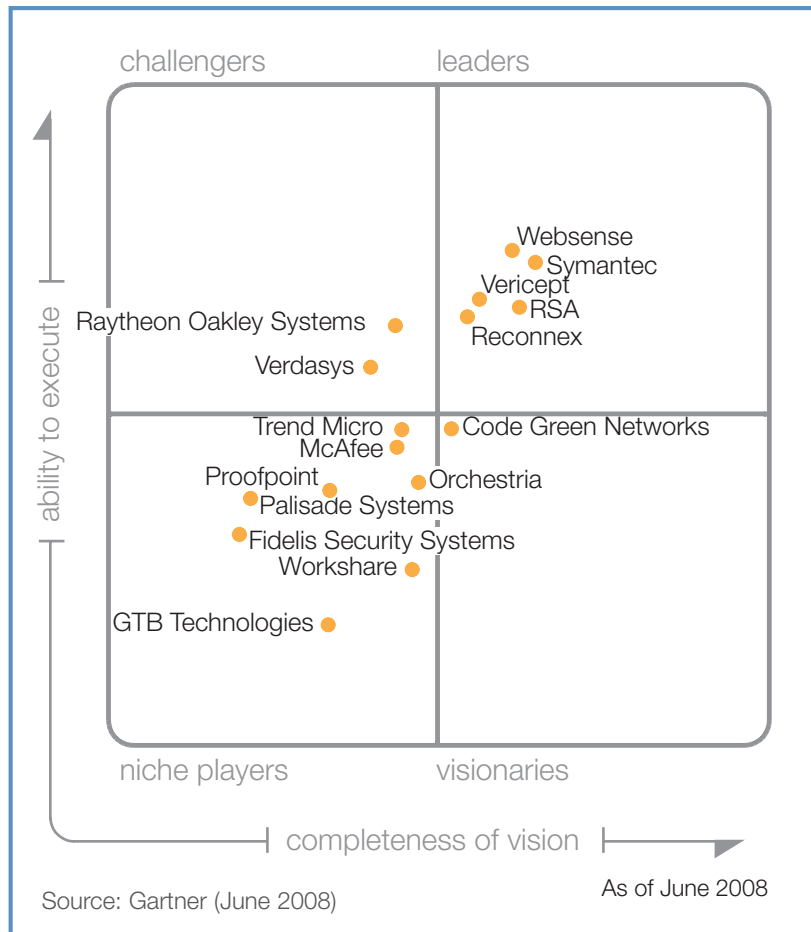
When referring to the DLP market, Gartner includes only content-aware DLP vendors, not the broader set of tools that can be used to address the disclosure of sensitive data using techniques such as file extension recognition and tagging technologies. Gartner's definition of DLP refers to tools used to prevent inadvertent or accidental leaks or exposure of sensitive enterprise information using content inspection technologies.

As noted earlier, the inclusion criteria of previous versions of this Magic Quadrant required, at a minimum, DLP network capabilities such as monitoring, filtering and blocking to qualify. Products that primarily offered endpoint or discovery DLP capabilities, but did not have the required network DLP requirements, were previously not included. Gartner adopted this strict criteria based on client inquiries and our own view of the market.

The 2008 update of the CMF/DLP Magic Quadrant was redesigned to include product offerings with support for one or more DLP capabilities, including monitoring, filtering and blocking of network communications, endpoint activities and data discovery capabilities. The 2008 Magic Quadrant gives higher rankings to more broadly capable offerings with greater depth of integration.

This shift in analytical perspective comes in response to growing demand from Gartner's clients for offerings that provide a suite of capabilities in place of dedicated network DLP solutions. This trend confirms Gartner's predictions, made in previous versions of this Magic Quadrant and elsewhere. We have long believed that integrated network, endpoint and data discovery capabilities – with a centralized management console capable of distributing a consistent set of policies, and providing usable event analysis and workflow for alerting on and remediating violations – was the ultimate goal and destination of this market.

Figure 1. Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention



The succession of acquisitions throughout 2007 also supports this view. The most noteworthy deals were the acquisitions of Onigma by McAfee, Port Authority by Websense, Tablus by RSA, Oakley Networks by Raytheon, Provilla by Trend Micro and Vontu by Symantec. The involvement of endpoint security suite vendors in the DLP market will continue to expand the endpoint capabilities and will drive greater integration of all services. Over time, this integration will commoditize and lower per-unit, basic DLP product pricing, bringing it more in line with standard premium offerings from the endpoint security suite vendors.

The Magic Quadrant is copyrighted June 2008 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2008 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

The 16 vendors that met Gartner's strict definition of this market – listed in this Magic Quadrant – provide many good choices for enterprises seeking content-aware DLP capabilities.

MAGIC QUADRANT

Market Overview

The maturing content-aware DLP market, which Gartner has identified in previous Magic Quadrants as the CMF or CMF/DLP market, now includes vendors of technologies for registering, finding, classifying, relocating, tagging and encrypting sensitive information – be it business-sensitive (business plans, account information or patent-pending ideas), employee-sensitive (HR information or benefits information), or regulatory- or policy-sensitive (the U.S. Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act or Payment Card Industry) – on enterprise networks, in storage arrays, in collaborative environments (such as SharePoint and Lotus Notes) and at endpoints. This is done to enforce policies, and to control the use and distribution of information within and beyond the enterprise boundary using protocol and activity reporting and blocking capabilities.

Traditional access control technologies only provide the ability to restrict access to sensitive information – they do not offer a layer of control once access has been provided. DLP, however, can restrict the use, as determined by policy, of sensitive information after access has been granted. These technologies use content inspection and will, in the near future, offer full integration with enterprise digital rights management (EDRM) tools, along with host-based encryption and other control technologies for enforcing policy.

These technologies are emerging as important information security and privacy controls. Among the key drivers of this market is the need to address varying mandates, including:

- Regulatory and commercial compliance requirements
- IT frameworks (organizational compliance)
- Governance – This market continues to experience rapid growth, but Gartner still considers it to be in its “adolescent” phase. The market's total value was an estimated \$50 million in 2006, and \$120 million in 2007. Gartner believes it will reach \$200 million to \$250 million in 2008.

A key factor in the ongoing maturation of solution and technology offerings has continued to be the infusion of significant amounts of

venture capital into relatively small vendors in 2006 and 2007. Many of these vendors have less than 100 employees, and received funding in the \$30 million to \$40 million range. During 2006 through 2007, several of these vendors were acquired by incumbent security players with solid positions in the larger security market. The DLP market continues to attract venture capital investment, even at this late stage, although most investing is being directed to existing solution providers.

One significant result of this market trend has been the accelerated development of core capabilities requested by clients within a given vendor's product set – specifically around support for an offering's previously unavailable features. Historically strong, network-only solution providers are now offering endpoint and discovery capabilities, and historically strong, endpoint-only solutions are broadening their offerings to include network and discovery capabilities.

Despite the growing preference for suite offerings, market adoption has continued to be influenced primarily by multichannel, network-monitoring requirements, which include FTP, e-mail, Telnet and instant messaging (IM). A clear increase in Gartner client inquiries and documented deployments also shows a trend toward deployments initiated at the endpoint. Gartner has also identified a trend toward products being deployed as part of enterprise initiatives to identify and find sensitive data residing on network shares, central data stores (such as network attached storage/storage array networks) and even local storage (such as laptop drives). These deployments are not as numerous as their network counterparts, nor as significant in terms of deal size; however, it is clear that 2008 will represent a tipping point in terms of deployment dollars.

Enterprises should expect significant market changes to continue throughout 2008. Gartner expects that some vendors will go out of business, while some of the stronger technology players will merge with others or be acquired by large, mainstream security vendors. Gartner expects two, or possibly three, additional deals to be announced in 2008.

Enterprises continue to use DLP technologies to develop, educate and enforce better business practices concerning the handling and transmission of sensitive data. This is a useful capability because, to date, most enterprises have failed to produce policies and processes that end users can be trusted to apply in a consistent manner.

Gartner believes DLP is emerging as an important information security control, with capabilities beyond those traditionally affiliated with monitoring. DLP assists management to identify and correct faulty business processes, identify and prevent accidental disclosures of sensitive data, and provide a mechanism for supporting compliance and audit activities. As such, many DLP tools offer hooks into identity and access management, document management, archiving systems and other content-rich sources, which will help to create a new market segment that addresses the requirements of compliance auditing. Several auditing firms have begun to employ these specific capabilities as part of their auditing programs, and Gartner believes this trend will continue throughout 2008 and beyond.

DLP tools continue to provide value in reducing accidental data leaks from the network and at the endpoint. However, these technologies continue to face challenges in dealing with deliberate attempts to circumvent corporate data-dissemination policies.

Gartner expects that the Microsoft Vista operating system will add complexity to endpoint deployments because of the system refresh cycle that is planned for many enterprises. Specifically, some vendor offerings may not support some of Vista's operating environments during the next 12 to 18 months, which will impact deployment schedules.

Despite the shift from a primary focus on network-based solutions to an integrated analysis of network, endpoint and discovery capabilities, the Leaders Quadrant for 2008 contains many of the same vendors as in past years. (Endpoint, discovery and network tools were weighted equally in this Magic Quadrant. Centralized management console capabilities, policy and sensitive content registration, and workflow tools were also assessed, but were not weighted as heavily as the other functions.) This is a testament to an aggressive product development cycle and a rapidly maturing lead- and sales-generation process.

The infusion of significant mainstream players into this market brings a strong potential for the integration of capabilities at many levels. For this reason, previously small, streamlined vendors will be challenged to hold their courses in the face of pressure to do too much during too short a time.

To accelerate development time and to make enhanced analytical capabilities part of their content inspection capabilities, vendors such as Palisade Systems, Proofpoint, Symantec/Vontu, Trend Micro and Websense have licensed and incorporated Autonomy's KeyView file-decoding engine. Although most also have licenses for Autonomy's Intelligent Data Operating Layer (IDOL) content

inspection, none implement these capabilities in their content inspection. Use of KeyView or IDOL should not be regarded as a negative, because they may provide a framework for consistent policy definition across vendor offerings in the future.

To remain in the Leaders Quadrant, vendors must be vigilant in enhancing all aspects of their products – including network, endpoint and data discovery capabilities – while significantly enhancing back-end workflow, management and integration with improved service capabilities.

Market Definition/Description

Gartner defines DLP technologies as those that – as a core function – perform deep content inspection of data at rest or in motion and can perform some level of remedial action based on policy settings, which can range from simple notification to blocking.

Products must support sophisticated detection techniques that extend beyond simple keyword matching (for example, advanced regular expressions, partial document matching, Bayesian analysis and machine learning).

The primary appeal of endpoint technologies will be among enterprises concerned with protecting intellectual property and other valuable enterprise data from theft. Network and discovery solutions' true value, by contrast, lies in helping management to identify and correct faulty business processes, and to identify and prevent accidental disclosures of sensitive data, as well as in providing a mechanism for supporting compliance and audit activities.

Inclusion and Exclusion Criteria

Vendors are included in this Magic Quadrant if their products:

- Detect sensitive content in any combination of network traffic and/or data at rest or endpoint operations.
- Detect sensitive content through the use of sophisticated, content-aware detection techniques, including, but not limited to, partial and exact document matching, structure data fingerprinting, statistical analysis, regular expression matching, conceptual and lexicon analysis, and keyword.
- Support the detection of sensitive data content in structured and unstructured data using registered and/or described data definitions.
- Analyze across multiple channels in a single product using a single management interface.
- Block, at minimum, policy violations that occur over e-mail communications.

- Are available as of December 2007.
- Are deployed in customer production environments, with at least five references.

Participants must be determined by Gartner to be significant players in the market via market presence or technology innovation, or both.

Vendors were excluded from this Magic Quadrant if:

- Products with simple data detection mechanisms support only keyword matching, lexicon or simple regular expressions.
- Network-based functions support fewer than four protocols (such as e-mail, IM or HTTP).

Added

- EMC/RSA (acquired Tablus)
- GTB Technologies
- McAfee
- Orchestria
- Raytheon Oakley Systems (acquired Oakley Networks)
- Symantec (acquired Vontu)
- Trend Micro
- Verdasys
- Workshare

Dropped

- Vontu (acquired by Symantec)
- Tablus (acquired by EMC/RSA)
- Oakley Networks (acquired by Raytheon Oakley Systems)

Vendors Considered but Not Included in This Magic Quadrant

- NextLabs
- Sendmail

Evaluation Criteria

Ability to Execute

Gartner weights a vendor's ability to execute heavily toward product capabilities, because most of the vendors in this adolescent market are still comparatively new. Our ratings are most influenced by three basic categories of capability network performance, endpoint performance and discovery performance.

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	standard
Market Responsiveness and Track Record	high
Marketing Execution	no rating
Customer Experience	high
Operations	high
Source: Gartner	

Completeness of Vision

The DLP market, although still comparatively new, is rapidly becoming mainstream in the U.S., and is gaining significant attention and traction in Europe and Asia. Many vendors were acquired in 2007 by endpoint security solution providers, and their offerings are becoming part of an overall product offering vision, along with acquiring greater breadth and depth of capabilities. However, the market remains intensely competitive and is becoming even more so, with four of the big endpoint antivirus vendors now fully engaged in the market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	no rating
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	standard
Geographic Strategy	no rating
Source: Gartner	

For this reason, Gartner gives strong preference to vendors that demonstrate completeness of vision – in terms of strategy for the future – and ability to execute on that vision. We continue to place a stronger emphasis on products than on marketing or sales strategies. A clear understanding of the business needs of DLP customers – even those that do not fully recognize those needs – 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.

Leaders

The leaders in this market have demonstrated a good understanding of client needs and offer comprehensive capabilities in all three functional areas, including network, discovery and endpoint directly or through well-established partnerships and tight integration. They offer aggressive road maps, but they will need to execute on those road maps, fully incorporate enhanced features being developed and address evolving market needs to remain in the Leaders Quadrant.

- Reconnex
- RSA
- Symantec
- Vericept
- Websense

Challengers

Two primarily endpoint-centric vendors are in the Challengers quadrant: Raytheon Oakley Systems and Verdasys. The future of their offerings will depend on the evolution of the endpoint marketplace and the vendors' ability to overcome the challenges associated with large, distributed endpoint deployments. The Verdasys product offering was analyzed according to publicly available and other Gartner sourced information.

Visionaries

There is only one product in the Visionaries Quadrant this year. Code Green Networks remains a visionary vendor because it provides a well-featured product set and continues to focus on small and midsize businesses (SMBs).

Niche Players

The Niche Players Quadrant is crowded, with many vendors competing for business with products that have meaningful credibility in mainly one network, endpoint or discovery DLP capability. Some vendors, such as Fidelis Security Systems, have strategic plans to offer "best of breed" products that address a single channel, while others, such as GTB Technologies, have

more-comprehensive, multichannel (endpoint, discovery and network) strategies, but still lack execution.

- Fidelis Security Systems
- GTB Technologies
- McAfee
- Orchestria
- Palisade Systems
- Proofpoint
- Trend Micro
- Workshare

Vendor Strengths and Cautions

Code Green Networks

Strengths

- Good network capability and baseline discovery and endpoint functions, with a primary focus on ease of use and products that serve the SMB market.
- Embedded message transfer agent functionality and flexible, native e-mail encryption capabilities via integration of Cisco/IronPort Systems and Voltage Security technology within the product, which adds significant value for SMBs that typically prefer integrated solutions.
- Some localization and support for double-byte characters (although presence outside the U.S. is limited).
- Positive reports from Code Green clients about their overall deployment experiences with the product and the level of support provided by the vendor.

Cautions

- Inability to scale to enterprise needs generally beyond 5,000 monitored users.
- Discovery capabilities are limited in scope and support.
- Product integration of OEM technology from Centennial Software is still a work in progress, although endpoint capabilities are becoming more defined.

Fidelis Security Systems

Strengths

- A strong network-based DLP offering.
- High-speed throughput and in-line network blocking.
- Strong presence and continuing appeal in the highly targeted U.S. federal government and Department of Defense market spaces.

- New infusion of venture funds and new leadership, providing hope that the company's offering will become more mainstream in focus and will appeal more to other target demographics.

Cautions

- Stated intention to remain entirely focused on network capabilities. Does not offer discovery or endpoint capabilities natively. Relies on partnerships to support endpoint capabilities commonly requested by clients.
- Has been content playing "catch up" in the past with other leading vendor offerings by choosing to build similar offerings instead of innovating in the market.
- Fidelis clients who require endpoint or data discovery DLP capabilities need to acquire solutions from alternate providers. Integration of multiple DLP solutions involves skilled staff familiar with select products to maximize value.
- Overly strong focus on, presence in and experience within the U.S. – and specifically the federal government and Department of Defense – limiting appeal to commercial banking, insurance, manufacturing and international enterprises.

GTB Technologies

Strengths

- Balanced network, discovery and endpoint portfolio.
- Ability to demonstrate innovation in partial document-matching algorithms (limited by low adoption).
- Promising market strategy, demonstrating that the company understands the needs of the DLP market.
- Product road map that addresses clearly identified market needs in network, discovery and endpoint functionality.

Cautions

- Continuing an early-stage focus on technology development and reference accounts, minimizing attractiveness until the company reaches a critical mass of client deployments.
- Execution and sales activity is typical of an early-stage vendor.
- Significant, competitive challenges from former startups acquired by large vendors that now possess formidable development and marketing capabilities, as well as market presence and awareness, will force the company to mature rapidly.

McAfee

Strengths

- Good endpoint and baseline network functionality.
- Worldwide presence, with a strong network of VARs that will appeal to large, geographically distributed organizations.
- Strong value for enterprise users of McAfee's market-leading endpoint solutions, and integration with McAfee ePO.
- Endpoint DLP solution provides a potential foundation for a good baseline of DLP capabilities for typical deployment requirements.
- Product road map has a defined focus on integration within McAfee's own environment. Enhancements to endpoint distribution of custom signatures will have broad appeal.

Cautions

- Lack of an overall comprehensive message and product capabilities with broader appeal, despite the company's understanding of the needs of its specific target market (its existing customer base).
- A more conservative product road map than some competitors, with limited addition of completely new functionality.
- Network support providing a baseline set of capabilities, but limited in environments with broader network DLP requirements.
- Discovery capabilities are not supported.

Orchestria

Strengths

- Good endpoint and discovery functions. Network DLP capability is typically deployed for messaging support.
- Core competency in separating message content from different internal groups (for example, buy- and sell-side communications).
- Strong overall customer satisfaction with offering's ability to address specific requirements around financial messaging DLP.
- Endpoint and discovery features and workflow are on par with the industry average in terms of integration, usability and workflow support for core competency.

Cautions

- Deployments are strongly focused on supporting financial services messaging content inspection (product features support wider use, but market penetration in the broader use cases is limited).
- Product road map shows significant enhancements to the entire capability set, but fully available products are not yet delivered.

Palisade Systems

Strengths

- Good network-centric DLP, combined with Web filtering, that supports agent-based discovery capabilities.
- Support for double-byte characters for content inspection (although interfaces are not localized to other markets).
- Usable workflow, which Gartner clients report integrates well in their environments.
- Support for enforcing network segmentation communication policies via DLP is unique among all vendors.

Cautions

- Weak, network-only-focused product road map that follows the market but demonstrates limited innovation or feature leadership.
- Small vendor with limited DLP deployments, which appeals to specific deployment scenarios.

Proofpoint

Strengths

- Provides good network-only capabilities.
- One reference reports that the product works well for its e-mail-centric deployments.

Cautions

- Lack of support for broader discovery and endpoint capabilities forces clients to deploy other DLP solutions to meet some enterprise needs.
- Product road map does not address broader market trends other than through partnerships.

Raytheon Oakley Systems

Strengths

- Strong endpoint solution (although complementary network capabilities are average).
- Unique endpoint capability for recording PC/Windows screen activity when an operation on sensitive content is detected.
- Good choice for enterprises with a strong need to protect high-value intellectual property.
- Large company with a worldwide presence that will appeal to geographically diverse enterprises.

Cautions

- DLP offering and sales, to date, have been highly U.S.-centric, with a strong focus on U.S. federal government and Department of Defense market segments.
- Discovery capabilities are not available at this time.
- Organizations must have a good privacy program in place to consider Raytheon Oakley Systems because of the nature of the product's recording capabilities.

Reconnex

Strengths

- DLP offering provides strong network and discovery components. The endpoint is sourced from Trend Micro and resold under Reconnex's label, and has early-stage integration with the rest of the offering.
- Unique capability to help enterprises understand their sensitive data through data mining and historical trending.
- Good workflow support.
- DLP scanning-only appliance is available as a separate product offering (Data Loss Profiler); expected to have broad appeal for enterprises with audit data management requirements.

Cautions

- As a small company with significantly larger competitors, Reconnex will have to continue to work diligently to pursue the growth trend in its customer base.
- Likely acquisition target in 2008.
- Lack of international presence or partnerships necessary to adequately leverage non-U.S.-centric opportunities.

RSA

Strengths

- Comprehensive network, endpoint and discovery offering that addresses all DLP elements demanded by a broad range of clients in all sectors.
- Strong described content capabilities enabled by formal knowledge-engineering processes, which provide a range of DLP inspection capabilities that are complementary to native document-fingerprinting content inspection capabilities.
- Strong geographic reach that will appeal to geographically diverse clients, but deployment scenarios will continue to be limited due to lack of double-byte support and localization.
- Support for distributed discovery agents, with broad appeal for enterprises that want to address complex discovery requirements across thousands of endpoints.

Cautions

- Best known for infrastructure solutions, with its endpoint offering continually being challenged by endpoint-centric and antivirus vendors.
- Aggressive and challenging road map, with significant integration plans beyond simple endpoint, network and typical discovery features – includes a broad range of EMC/Documentum/RSA and other integrations. Although current efforts show great promise, complexity may impact delivery; therefore, Gartner remains optimistic but cautious.

Symantec

Strengths

- Strongest network and workflow capabilities, balanced by discovery and relatively new endpoint capabilities.
- Global presence, with a strong VAR network that appeals to large, geographically distributed enterprises.
- Integration of DLP capabilities within the existing Symantec security offering will simplify DLP endpoint deployments among clients that are already Symantec antivirus customers.
- Aggressive product road map, demonstrating a clear understanding of the broad DLP market requirements.

Cautions

- Lack of localization, thus limiting deployment scenarios.
- Poor record of integrating past acquisitions, which will require considerable vigilance about properly managing its DLP acquisition to remain in the Leaders Quadrant.
- Need for customers to verify execution against an aggressive road map.

Trend Micro

Strengths

- Offering has strong endpoint capabilities, but possesses only average discovery capabilities and no network functionality.
- Global presence, with a strong network of VARs that will appeal to large, geographically distributed organizations.
- Integration of DLP capabilities within the existing Trend Micro security offering will simplify DLP endpoint deployments among clients that already are Trend Micro antivirus customers.
- Strong, well-executed product road map (although its vision continues to be focused on the endpoint, thus limiting adoption in large accounts).

Cautions

- Lack of network and e-mail capabilities in the company's offering limits its appeal within large accounts, although we expect that this will be addressed in future releases.
- Endpoint product needs enhancements to its content awareness and blocking capabilities to better compete against those planned by other large endpoint security solution providers.

Verdasys

Strengths

- Strongest endpoint function included in this Magic Quadrant; however, its offering has limited discovery and no network capabilities.
- History of innovation with an agent that has a broad appeal among enterprises that require strong controls on intellectual property.

- Support for double-byte characters, with client deployments supporting a global strategy – factors that should appeal to large, diverse global enterprises.

Cautions

- DLP functions are not available for unmanaged systems, with no plans to develop network-based capabilities.
- Organizations requiring the full breadth of DLP deployments must continue to rely on partners to fulfill this mandate.
- Scalability challenges for some deployments.
- Lack of vision to address broader market requirements, despite a strong road map for core functions.

Vericept

Strengths

- Strong network, discovery and endpoint DLP capabilities, along with good workflow.
- Use of the Content Analysis Description Language (CANDL) appeals to enterprises that want to register unique and specific content for DLP inspection.

Cautions

- Lack of localization and double-byte character support limits the appeal to large enterprises and international markets.
- Likely acquisition candidate.
- One of the few-remaining small, independent vendors – needs to work diligently to enhance its product offering, ensure relevance in the overall market and grow market presence.

Websense

Strengths

- Strong network and discovery capabilities, along with baseline endpoint and good workflow support.
- Global presence, with a strong network of VARs, which appeals to large, geographically distributed enterprises.

- Integration of DLP capabilities within the existing Websense security offering will simplify DLP deployments among clients that are already Websense customers.
- Strong product road map that was well-executed in 2007; demonstrates the company's ability to effectively integrate new features within existing product sets.

Cautions

- Although the DLP product portfolio shows strong overall capabilities, the offering continues to appeal mostly to the existing Websense client base, which wants to leverage existing, deployed products and tools.
- New endpoint functionality will continue to be challenged by larger and more-endpoint-centric vendors.

Workshare

Strengths

- Good endpoint, with baseline network, discovery and workflow capabilities.
- Has demonstrated maximum value with existing clients of its product suite, primarily in the legal work domain.
- Well-built DLP product suite that fully integrates with the rest of the offerings in the Workshare portfolio. Additional capabilities include selectable encryption options; EDRM support; and third-party, encrypted e-mail capabilities.

Cautions

- DLP solution deployments are still in the early stages.
- Needs to develop a broader appeal among nontraditional client base to significantly expand and grow market share.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Acronym Key and Glossary Terms

CMF	content monitoring and filtering
DLP	data loss prevention
EDRM	enterprise digital rights management
ePO	ePolicy Orchestrator
IDOL	Intelligent Data Operating Layer
IM	instant messaging
SMB	small and midsize business
VAR	value-added reseller

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.