Magic Quadrant for
Content-Aware Data Loss Prevention

The maturing market for content-aware data loss prevention technologies has experienced another year of significant industry consolidation. Enterprisewide capabilities have become more broadly available, but the market is only now reaching the end of its "adolescent" phase.

WHAT YOU NEED TO KNOW

This document was revised on 25 June 2009. For more information, see the Corrections page on gartner.com.

The market for content-aware data loss prevention (DLP) continues to show significant market growth despite difficult worldwide economic conditions. The reasons for the continuing strength of this market include the growing maturity of the available content-aware DLP technologies and buyer awareness that these technologies can help address regulatory compliance requirements, which are actually increasing in the downturn.

Many vendors of products unrelated to DLP are embedding content-aware DLP technologies in their suite offerings. One indication of this trend is a significant amount of merger and acquisition (M&A) activity and other consolidation in this market, which Gartner expects to continue. In making their business decisions, businesses should consider that, by 2011, the broad availability of content-aware endpoint protection platform (EPP) components will result in the commoditization of endpoint DLP, and Gartner expects prices for endpoint DLP agents to drop by 50%. While pricing is expected to drop, adoption of endpoint content-aware DLP will rise significantly during this time period, which will result in a continued increase in the overall market size for endpoint content-aware DLP.
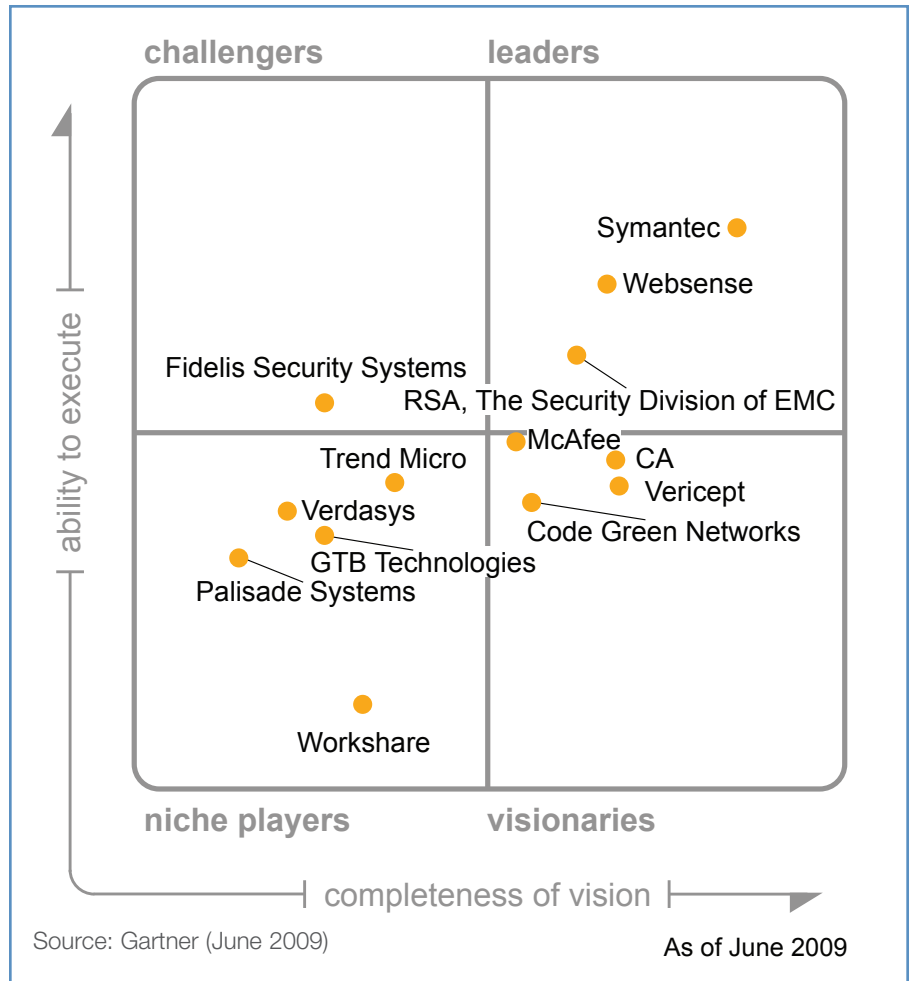
MAGIC QUADRANT

Market Overview

Gartner uses the term "content-aware DLP" to describe a set of technologies and inspection techniques used to classify information content contained within an object (for example, a file, an e-mail message, a packet, an application, or a data store while at rest [in storage], in use [during an operation] or in motion [across a network]). It also describes the ability to dynamically apply a policy (for example, by logging, reporting, classifying, relocating, tagging, encrypting or applying enterprise digital rights management [EDRM] protections). Mechanisms for classifying information content may include exact data matching, structured

Gartner

data fingerprinting, statistical methods (such as Bayesian and machine learning), rule and regular expression matching, published lexicons, conceptual definitions, keywords, and watermark recognition. Enterprises generally understand the need to use DLP technologies to develop, educate and enforce better business practices concerning the handling and transmission of sensitive data.

Many content-aware DLP vendors have made improvements designed to facilitate configuration, baselining and sensitive content registration. However, the effort required to operate and maintain content-aware DLP deployments beyond basic configurations varies widely from vendor to vendor. Gartner inquiry data shows that many enterprises are still struggling 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 vendor offerings against independently developed, enterprise-specific requirements.

There are three primary content-aware DLP channels: network host/endpoint and discovery (of stored data).This Magic Quadrant evaluates single-channel vendors that offer only one of the primary channels as well as enterprise DLP vendors that offer all three channels, with workflow and management functions to support all three. The scoring system used does not typically penalize single-channel vendors, such as the network-focused Fidelis Security Systems and the endpoint-only Verdasys, but the Leaders quadrant contains only enterprise DLP vendors for 2009. Vendors that wish to remain in the Leaders quadrant will need to be vigilant in continuing to enhance all aspects of their products – including network, endpoint and data discovery capabilities – while significantly enhancing back-end workflow and management as well as integration with improved service capabilities.

Content-aware DLP technologies are emerging as important information security and privacy controls. One of the key drivers of adoption in this market is the need to address a broad range of mandates, including:

• Regulatory and commercial compliance requirements

• IT frameworks (for organizational compliance)

• Governance

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

Source: Gartner (June 2009)

As of June 2009

This market continues to experience rapid and steady growth, with an estimated total gross revenue of $50 million in 2006, $120 million in 2007 and $215 million in 2008. Content-aware DLP deployments and overall sales have been only minimally affected by the current economic downturn. Gartner believes this market will reach $300 million in 2009, but is still in its "adolescent" phase. A key factor in the ongoing maturation of the market for content-aware DLP technology offerings and the offerings themselves has been the acquisition of small, venture-capital-backed startups by large security suite vendors. These large vendors are able to support complex development life cycles and have extensive sales, partner and reseller networks that can deliver content-aware DLP offerings to more-varied client deployment environments.

More vendors of non-DLP-related products – for example, e-mail, intrusion detection and identity and access management (IAM) technologies – added or enhanced single-channel content awareness to their products in 2008. The embedding of content awareness 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 content-aware enterprises. Enterprise DLP vendors will support application programming interfaces (APIs) that can manage common detection policies and response workflows by 2012.

The market for content-aware DLP also continues to experience significant M&A activity, with eight acquisitions since 2006:

- CA's acquisition of Orchestria in 2008

- McAfee's acquisitions of Onigma in 2006 and Reconnex in 2008

- Raytheon's acquisition of Oakley Networks in 2007

- The acquisition of Tablus by RSA, The Security Division of EMC in 2007

- Symantec's acquisition of Vontu in 2007

- Trend Micro's acquisition of Provilla in 2006

- Websense's acquisition of PortAuthority in 2007

Another important content-aware DLP vendor development was Microsoft's 2008 announcement of a partnership to incorporate RSA, The Security Division of EMC's content-aware DLP functionality in its products. Gartner expects more acquisition and other consolidation activity through 2009, but we believe this market is nearing the end of the acquisition cycle. We expect a few more acquisitions in 2009 and 2010, with the remaining small startups either merging with larger vendors or exiting the market (see Note 1).

Note 1

Changes in the Market

An important recent development is the full entry of IAM vendors into this market, which had primarily interested security suite vendors. RSA, The Security Division of EMC completed its acquisition of Tablus nearly 18 months ago, and until CA's acquisition of Orchestria in January 2009, the Microsoft/RSA/EMC partnership represented the only content-aware DLP offering by an IAM vendor. Gartner believes other IAM suite vendors have acquisition and partnership plans in the works. We anticipate a splitting of market offerings between security suites and IAM vendor offerings, which will give enterprises a better choice when acquiring content-aware DLP products, based on their internal buying center focus. The classification and tagging capabilities of content-aware DLP, for example, hold particular promise for IAM when combined with the contextual awareness that is exhibited by role life cycle management and entitlement tools to enable the detailed definition of policies (rules) for access. Content and context play critical roles in permitting technical access policymakers more flexibility in defining, assigning and enforcing entitlements for access to content and other resources.

Customer adoption of content-aware DLP has continued at a steady pace among early adopters, typically enterprises with rigorous regulatory compliance requirements or serious concerns about intellectual property protection. The resiliency of this market in the face of difficult economic conditions is due in part to many enterprises acquiring content-aware DLP functionality as part of larger governance and compliance initiatives, which have actually taken on greater importance as a result of the downturn. Concerns about threats to intellectual property resulting from employee downsizing have been documented as a factor influencing content-aware DLP deployments. Content-aware DLP offers the capabilities to broadly identify compliance data and apply remedial actions to ensure that data is protected as required by policy. However, Gartner has not seen a significant increase in purchases of content-aware DLP solutions to specifically address this as a primary concern.

Gartner client inquiries in 2008 indicated that 45% of enterprises led their content-aware DLP deployments with network requirements, with 30% beginning with discovery requirements and 25% with endpoint requirements. Enterprises that began with network or endpoint capabilities nearly always deploy data discovery functions next. Approximately 20% of enterprises purchase full-suite channel coverage, but few deploy all three simultaneously.

Gartner expects the Microsoft Vista and Windows 7 operating systems (OSs) – and many enterprises' planned OS refresh cycles – to continue to add complexity to endpoint deployments. This is due to the system refresh cycle that is planned for many enterprises. Some vendor offerings may not support some aspects of the Vista or Windows 7 operating environments through late 2010, and this fact will affect deployment schedules.

To accelerate development time and to make enhanced analytical capabilities part of their content inspection capabilities, vendors including Palisade Systems, Proofpoint, Symantec/Vontu, Trend Micro and Websense have licensed and incorporated Autonomy's KeyView file decoding engine. Some also have licenses for Autonomy's Intelligent Data Operating Layer (IDOL) content inspection. However, none have yet implemented the IDOL capabilities in their content inspection. The use of KeyView or IDOL should not be regarded as a negative, because it may, at some point in the future, provide a framework for consistent policy definition across vendor offerings. It is important to note that this has yet to materialize itself in current product road maps.

Market Definition/Description

Gartner defines content-aware 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 – ranging from simple notification to active blocking – based on policy settings. To be considered as a content-aware DLP technology, 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).

Gartner research continues to indicate that the primary appeal of endpoint technologies will be to 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 providing a mechanism for supporting compliance and audit activities.

Inclusion and Exclusion Criteria

Vendors were included in this Magic Quadrant if their offerings:

- 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, structure data fingerprinting, statistical analysis, regular expression matching, conceptual and lexicon analysis, and keywords

- 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 over e-mail communications

- Were generally available as of 31 December 2008

- 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 were 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)

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 2009)	

Added

- CA

Dropped

- Orchestria (acquired by CA)

- Reconnex (acquired by McAfee)

- Raytheon/Oakley Networks (no longer in the content-aware DLP market)

- Proofpoint (no longer in the content-aware DLP market)

Evaluation Criteria

Ability to Execute

Gartner weights ability to execute (see Table 1) heavily toward product capabilities, because most of the vendors in this adolescent market are still comparatively new as venture-funded startups or as part of a relatively recent acquisition that has yet to yield significant leveraging of capabilities integration as part of a larger product portfolio. Our ratings are most influenced by three basic categories of capability: network performance, endpoint performance and discovery performance. Innovation in pure content-aware DLP capabilities was highly valued in this Magic Quadrant, because this market is reaching stasis in terms of content detection technologies and protocol analysis. 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.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	Standard
Geographic Strategy	Standard
Source: Gartner (June 2009)	

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 (see Table 2). 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 quadrant has only three vendors for 2009, because this market continues to evolve. The leaders have demonstrated good understanding of client needs and offer comprehensive capabilities in all three functional areas – network, discovery, and endpoint – either directly or through well-established partnerships and tight integration. They offer aggressive road maps, and they will need to execute on those road maps, fully incorporate enhanced features currently in development and address evolving market needs to remain in the Leaders quadrant. The leaders are:

• RSA, The Security Division of EMC

• Symantec

• Websense

Challengers

Fidelis Security Systems is in the Challengers quadrant – the only vendor to achieve this status for 2009 – based on execution and success as a best-of-breed single-channel DLP vendor. Gartner believes Fidelis is unlikely ever to enter the Leaders quadrant, which favors enterprise DLP vendors that address all three primary DLP deployment channels (network, discovery and endpoint).

Visionaries

The four vendors in the Visionaries quadrant have very different backgrounds in this market. CA, following its acquisition of Orchestria, has good vision and the potential to rise into the Leaders quadrant next year with strong execution on its road map and sales. Code Green Networks, which has a quality offering for small and midsize businesses (SMBs), has released an enterprise version but lacks a track record of success with larger enterprises. McAfee acquired Reconnex, which was in the Leaders quadrant in 2008; integration challenges have caused Gartner to position McAfee as a visionary for 2009, but with some effective execution on its road map execution, the company should be back in the Leaders quadrant in 2010. Vericept, one of the few remaining independent vendors in this market, has experienced execution challenges and has, therefore, been downgraded from leader to visionary.

Niche Players

The Niche Players quadrant has five vendors for 2009. GTB Technologies and Palisade Systems are small startups that continue to play "catch-up." Trend Micro has shown some innovation, but has yet to publicly articulate a comprehensive vision for its approach to DLP. Verdasys was a challenger last year, but has suffered from lack of focus and visibility in this market. Trend Micro is working at developing broad content-aware DLP capabilities, but currently only offers endpoint-content-aware DLP. Workshare has competitive features but has not been able to execute in terms of sales or production deployments for content-aware functions.

Vendor Strengths and Cautions

CA

CA acquired stand-alone DLP vendor Orchestria on 5 January 2009, and has rebranded its product as CA DLP.

Strengths

- It has good endpoint and discovery functions, with network DLP capability historically deployed for messaging support.

- It has forward-looking vision, including the integration of content-aware DLP capabilities with CA's governance, security information and event management (SIEM), and identity and access management (IAM) offerings.

- It has proven competency in delivering content-aware DLP capabilities for messaging infrastructures and isolating sensitive content within different regulatory compliance domains (for example, buy/sell communications and advisory services communications).

- It has significant scalability and a strong client base in financial services, yielding advanced content-aware DLP feature support, specifically around messaging infrastructures such as Bloomberg alerts.

- It has global reach, appealing to large, geographically diverse enterprises.

Cautions

- Orchestria has few full-suite enterprise DLP deployments outside of financial services.

- Through 2009, CA will face challenges to understand and support the enterprise DLP market beyond Orchestria's traditional installed base in financial services while executing on CA's broader vision to integrate CA DLP with IAM and SIEM. However, the first six months post-acquisition have gone smoothly.

Code Green Networks

Code Green's proven strength remains an easy-to-use, low-cost content-aware network DLP for organizations with fewer than 2,500 monitored people; however, in 4Q08 it delivered its first enterprise version to support enterprises with more than 5,000 people.

Strengths

- It has good network capabilities and baseline discovery functions, with a primary focus on ease of use and a proven track record with smaller businesses (fewer than 2,500 users).

- It has an offering that now addresses the content-aware DLP needs of enterprises (organizations with more than 5,000 users) beyond Code Green's traditional SMB focus. This makes the overall offering attractive to price-sensitive enterprise buyers.

- It has embedded message transfer agent (MTA) functionality and flexible native e-mail encryption capabilities via integration of Cisco/IronPort Systems as well as Voltage Security technology within the product. This adds significant value for SMBs, which typically prefer integrated solutions.

- It has support for double-byte characters and some localization.

- Its pricing is competitive.

Cautions

- Its new endpoint agent is very early stage and lacks competitive features, such as blocking.

- It has no track record of large enterprise deployments.

- Its discovery capabilities are limited in scope and support.

- It has limited presence and support outside the United States.

Fidelis Security Systems

Fidelis's XPS product line offers one of the strongest single-channel (network) content-aware DLP offerings; however, it does not offer endpoint capabilities and has very limited network-centric passive discovery capabilities.

Strengths

- It has a strong and highly scalable network-content-aware DLP offering that addresses the needs of large enterprises looking for network-only capabilities.

- It is differentiated by high-speed throughput and in-line network blocking.

- It has strong presence and continuing appeal for U.S. government/Department of Defense customers.

- It has an IBM reseller relationship (that also includes the Verdasys content-aware endpoint agent and server agent DLP offering), which brings credibility and reach to a small, venture-funded vendor, giving it visibility and deployment opportunities.

Cautions

- Its stated intention to offer only network DLP reduces the company's appeal to organizations looking for comprehensive enterprise DLP capabilities.

- Its best-of-breed functions are appropriate to U.S. government/ Department of Defense buyers, but may not be strong differentiators in other market segments, such as commercial banking, insurance, manufacturing and international enterprises.

- Its customers outside the United States must go through IBM Global Services for support.

GTB Technologies

GTB is a small vendor focused on DLP for small and midsize businesses, such as credit unions.

Strengths

- It has a balanced network, discovery and endpoint portfolio, with a good price point for smaller organizations.

- It has promising innovations in partial document matching algorithms.

- GTB has shifted its sales model to focus on small and midsize businesses in financial services.

Cautions

- It is an early-stage company offering aggressive pricing.

- Its endpoint DLP capabilities are limited to controlling data transfer to removable media and lack self-remediation.

McAfee

McAfee acquired stand-alone DLP vendor Reconnex in September 2008. While some integration progress has been made, McAfee will be challenged through 2009 to effectively integrate the Reconnex DLP capabilities with its existing endpoint.

Strengths

- Its acquisition of Reconnex, which brought McAfee much-needed content-awareness functions, should, over time, be incorporated into a comprehensive enterprise DLP offering.

- It has worldwide presence, with a strong network of value-added resellers (VARs), which appeals to large, geographically distributed enterprises.

- It offers strong value for current enterprise users of McAfee's other endpoint solutions (for example, antivirus tools).

- It has native file folder disk and e-mail encryption capabilities.

- Its endpoint presence and network infrastructure (e-mail Web gateway firewall and IPsec) are all managed by its ePolicy Orchestrator (ePO), which can lower the cost of deployment for existing McAfee clients.

Cautions

- The very rapid pace of McAfee acquisitions during the past 12 months is making it difficult for McAfee to properly digest and leverage its newly acquired talent and technical capabilities.

- Its separate network, endpoint and data discovery products are not completely integrated with McAfee's core ePO offering.

- Despite McAfee's comprehensive view of content-aware DLP, there is a continuing lack of integration among content-aware DLP endpoint, network and discovery capabilities, specifically in support of centralized management, policy and content-aware DLP engines within various McAfee product offerings.

Palisade Systems

Palisades's content-aware DLP offering combined with URL filtering, instant messaging (IM) proxy, application filtering and e-mail/Web proxy supports agent-based discovery capabilities at a very competitive, SMB-friendly price.

Strengths

- It has new management oversight and investment, which should positively influence product development and focus its marketing resources on growing the company's SMB network-centric DLP offering.

- It supports double-byte characters in content inspection, making it useful for detection of non-English-language content. While Palisade has clients outside of North America, its current primary sales focus continues to be in North America.

- It demonstrates ease of deployment and use, as reported by Gartner clients.

Cautions

- Its road map follows the large enterprise market, which limits the appeal of the solution to SMBs with minimal requirements.

- There is some vendor risk because Palisade is playing catch-up with larger, more mature, vendors and also is competing with other SMB-focused independent solution providers.

RSA, The Security Division of EMC

DLP Suite from RSA, The Security Division of EMC supports comprehensive enterprise content-aware DLP functions demanded by a broad range of clients.

Strengths

- Its complete, comprehensive network, discovery and endpoint offering that addresses all the DLP elements demanded by a very broad range of customers across all sectors.

- It has strong described-content capabilities enabled by formal knowledge-engineering processes, providing a broad range of DLP inspection capabilities that are complementary to native document fingerprinting content-inspection capabilities.

- Its global reach will appeal to geographically diverse clients.

- Its support for distributed discovery agents, with broad appeal for enterprises that wish to address complex discovery requirements across thousands of endpoints.

Cautions

- Its limited double-byte and localized support continues to hamper international sales as well as sales to large, geographically dispersed multinational enterprises.

- It is best-known for network and discovery content-aware DLP infrastructure solutions, with an endpoint offering that will continue to be challenged by endpoint-centric and antivirus vendors.

Symantec

Symantec Data Loss Prevention continues to be the strongest overall enterprise DLP capability; however, it has the highest license costs in the market.

Strengths

- It has industry-leading network and workflow capabilities, balanced by competitive discovery and endpoint capabilities.

- Its continuing strength in content-aware DLP business follows its well-executed Vontu acquisition.

- Its global presence, with a strong VAR network, will appeal to large, geographically distributed enterprises.

- It supports double-byte characters and localized Microsoft Windows operating systems (OSs) in 16 languages.

- It has an aggressive product road map and execution, demonstrating a very clear understanding of broad DLP market requirements.

- It has a very mature deployment methodology model that is unique in this market and – according to Gartner clients – a key influence in the decision-making process.

- Symantec, as a strategic vendor in storage, endpoints, e-mail and Web gateways, has a significant advantage and customer reach.

Cautions

- Vontu 9 endpoint agent (released in December 2008) is more competitive than earlier releases.

- It has the most expensive full-suite enterprise license costs.

- Its administrative console is not localized, and this may hamper deployment scenarios in non-English-speaking environments.

Trend Micro

Trend Micro's LeakProof offers competitive endpoint capabilities, but continues to possess only below-average discovery capabilities and no network functionality.

Strengths

- It has strong endpoint capabilities.

- Its global presence, with a strong network of VARs, will have appeal to geographically distributed large enterprises and midsize businesses.

- Its proprietary partial document match hash algorithm yields significant efficiency.

Cautions

- Its average content-aware discovery capabilities and lack of content-aware network and e-mail capabilities, limits Trend Micro's appeal to large accounts looking for a comprehensive enterprise DLP solution.

- Despite Trend Micro plans to develop and integrate content-aware DLP into its existing products, little progress has been demonstrated to date.

- Its endpoint product requires enhancements to content-awareness and blocking capabilities to be competitive.

- Its loss of two key content-aware DLP partners (Reconnex, acquired by McAfee, and Utimaco, acquired by Sophos) negatively affects its competitiveness.

Verdasys

Verdasys's strong endpoint control product has content-aware functions.

Strengths

- Its solution is appealing to enterprises that require strong controls for the protection of intellectual property.

- Its support for double-byte characters, with client deployment supporting a global strategy.

- Its IBM reseller relationship (which also includes the Fidelis content-aware network DLP offering) brings credibility and reach to this small, venture-funded vendor, giving it visibility and deployment opportunities.

Cautions

- Its endpoint functionality is no longer market-leading, due to significant endpoint investment by competitors and its shift of focus to other product lines.

- It has limited appeal outside of high-end control deployments due to lack of content-aware DLP support for unmanaged systems.

- Its high pricing will result in a loss of competitiveness as endpoint DLP functions become commoditized.

- It needs to continue to rely on partners to fulfill the mandates of enterprises that require the full breadth of DLP deployments.

- There have been continuing reports of scalability and platform challenges for some complex, diverse deployments.

Vericept

Vericept is one of the few remaining stand-alone enterprise DLP vendors that have all the necessary components to address network, endpoint and discovery use cases. However, it is a likely acquisition candidate and has struggled during the past year with execution as the market consolidates.

Strengths

- It has strong network, discovery and endpoint DLP capabilities, as well as good workflow.

- Its support for endpoint agent and a discovery software-as-a-service (SaaS) model for content-aware DLP is unique in the industry and at a price point that will make it very competitive with traditional content-aware DLP deployments.

- Its SaaS offering will appeal to organizations that require very capable content-aware DLP, but are unable to install or maintain hardware-/software-based offerings.

- Its use of Content Analysis Description Language (CANDL) offers significant appeal to enterprises that wish to register unique and very specific content for DLP inspection.

- Its aggressive, highly competitive pricing results in wins of accounts that normally could not afford this level of feature-rich, content-aware DLP capabilities.

Cautions

- It has minimal localization and double-byte character support, limiting its appeal for large enterprises and international markets.

- There is vendor risk associated with ongoing efforts to rescale the business. This affects company operations, product development and partnership plans.

- As one of the last independent full-suite enterprise DLP vendors, it is a likely acquisition candidate. Acquisition would represent challenges as well as benefits to Vericept and its customers.

- Competitive pressure from large antivirus vendors is beginning to affect Vericept's ability to gain presence into established antivirus accounts.

Websense

Websense provides a comprehensive enterprise DLP capability through its Data Security Suite, which has all the components necessary to address network, endpoint and discovery use cases.

Strengths

- Its strong network, discovery and endpoint capabilities, along with good workflow, offer customers a very competent and well-rounded content-aware DLP solution.

- Its global presence, with a diverse network of VARs, appeals to large, geographically distributed enterprises.

- It leads with subscription pricing, but offers perpetual licensing for clients who require it.

- Its integration of DLP capabilities within the existing Websense Web Security Gateway, simplifies content-aware DLP deployments for current Websense customers upgrading to this product.

- It has a strong, content-aware DLP product evolution road map, with good execution in 2007 and 2008.

Cautions

- It has an offering that is most appealing to current Websense clients wishing to leverage already-deployed products.

- It continues struggling to achieve significant sales success against competing incumbent endpoint antivirus vendors, despite consistently making shortlists for content-aware DLP RFIs/RFPs.

Workshare

Workshare has announced its intent to position its capabilities away from the pure-play DLP market into a supporting role for its core competencies, such as metadata cleansing and its target market – law firms.

Strengths

- Its endpoint, network and discovery content-aware DLP capabilities provide current Workshare customers with a relatively simple deployment path for incorporating content-aware DLP.

- Law firms using Workshare core competencies (such as metadata cleansing) should consider Workshare for complementary DLP functions.

Cautions

- It is unable to provide enterprise content-aware DLP production deployment references.

- It is primarily relevant to current Workshare customers.

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.

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 and skills, 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 that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales 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 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 initiatives, 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 and so on.

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 to 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 products 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 sets 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 vertical markets.

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.