Magic Quadrant for Content-Aware Data Loss Prevention

Gartner RAS Core Research Note G00200788, Paul E. Proctor, Eric Ouellet, 2 June 2010, RV4A306062011

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 (SWGs) 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

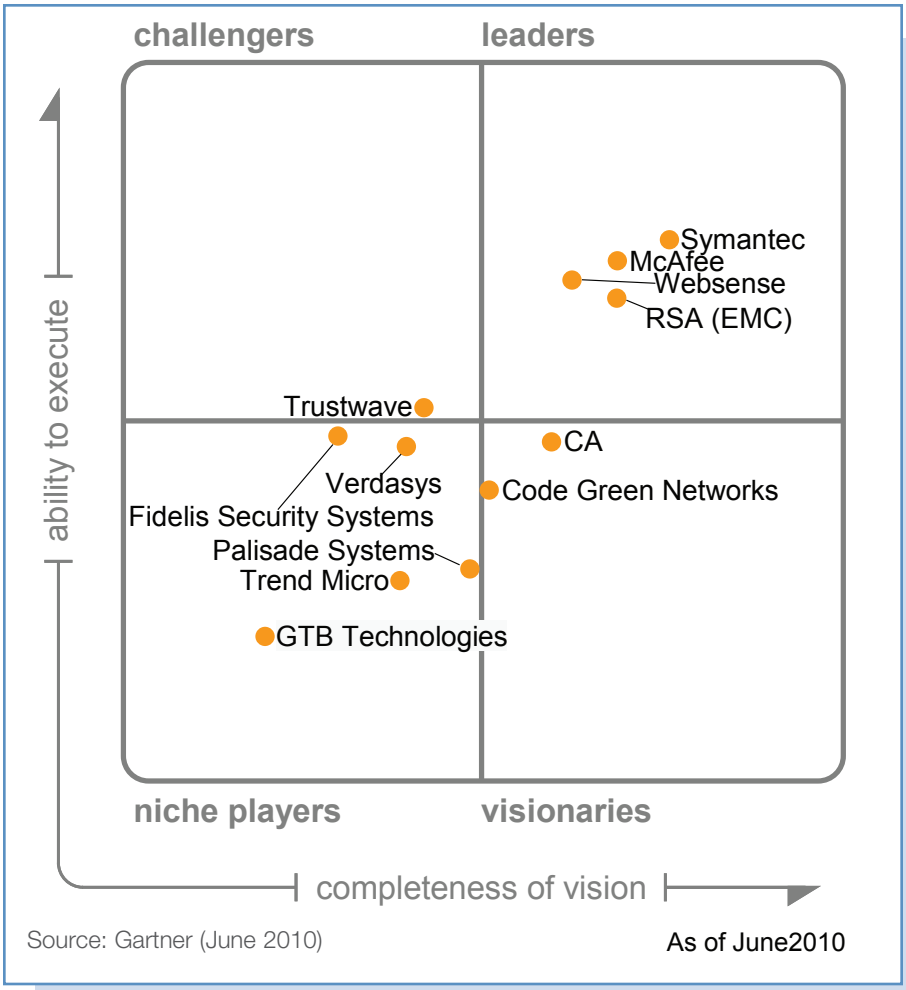
Gartner

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.

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



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 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 though 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)	

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 2010)	

Leaders

The Leaders quadrant has four vendors in 2010. The Leaders have demonstrated good understanding of client needs and offer comprehensive capabilities in all three functional areas — network, discovery and endpoint — 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:

- McAfee
- RSA (EMC)
- Symantec
- Websense

Challengers

Trustwave is in the Challengers quadrant based on the good capabilities of the product and the challenges presented by a business model that is not focused on the DLP market. Its ability to execute has gone up, but its vision is now limited. This is a significant change from 2009, when the Vericept product (acquired by Trustwave) was in the Visionaries quadrant.

Visionaries

The two vendors in the Visionaries quadrant have very different backgrounds in this market. CA has made steady gains in execution throughout 2009, but remains in the Visionaries space based on the lack of certain key features. Code Green Networks, which has a quality offering for small and midsize businesses (SMBs) and a handful of enterprise customers, lacks broad portfolio capabilities exhibited by the vendors in the Leaders quadrant.

Niche Players

The Niche Players quadrant has five vendors for 2010. GTB Technologies and Palisade Systems are small startups that continue to play "catch-up." Verdasys and Fidelis Security Systems provide best-of-breed technologies in endpoint and network functions respectively, but lack the comprehensive features and deployment configurations that many enterprises require. Trend Micro continues to develop broad content-aware DLP capabilities, but is still very early stage, with a lack of core offerings around network and discovery.

Vendor Strengths and Cautions

CA

CA DLP has good endpoint, discovery and network DLP capability, but lacks some common functions found in other products — such as partial document match. CA has successfully expanded the appeal of the product beyond its roots in financial services, making it more broadly applicable to all industries seeking enterprise DLP. CA DLP is a strong product that will be competitive to products in the Leaders quadrant in many situations.

Strengths

- It has forward-looking vision, including the integration of content-aware DLP capabilities with CA's log management and identity and access management (IAM) offerings.
- It has a proven competency in delivering content-aware DLP capabilities for isolating sensitive content within different regulatory compliance domains.
- It is scalable and has advanced content-aware DLP features support, with proven capability around messaging infrastructures.
- CA has global reach, appealing to large, geographically diverse enterprises.

Cautions

- The product does not support partial document match or other registered data detection mechanisms.
- CA has made progress, but continues to face challenges in the enterprise DLP market.
- The strength of the IAM/DLP vision and product features is balanced by a lack of experience with customers using these capabilities in production environments.

Code Green Networks

Code Green's proven strength remains in easy to use, low-cost, content-aware network DLP for organizations with fewer than 2,500 monitored people. It has delivered on the promise of a scalable enterprise version that retains its strength in ease of use and deployment. Network-DLP-focused organizations with up to 50,000 people should consider Code Green Networks.

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 is very easy to deploy and use for up to 50,000 users, making the overall offering attractive to price-sensitive enterprise buyers.
- Its embedded message transfer agent (MTA) functionality and flexible native e-mail encryption capabilities — via integration of ZixCorp Cisco/IronPort Systems secure envelope and Voltage Security VSN technology within the product — add significant value for SMBs, which typically prefer integrated solutions.
- It has support for double-byte characters, and some localization.

Cautions

- Its endpoint agent remains very early stage, and is not competitive with similar capabilities from other vendors.
- Its discovery capabilities are limited in scope and support.
- It has limited presence and support outside the U.S.

Fidelis Security Systems

Fidelis' XPS product line offers strong network content-aware DLP capabilities, but it does not offer endpoint capabilities and has very limited network-centric discovery capabilities. It has a strong differentiator focusing on the use of content-aware mechanisms to detect and address malicious code. It is a strong and highly scalable network content-aware DLP offering that addresses the needs of large enterprises looking for network-only capabilities. Fidelis' move into the Niche Players quadrant is not based on any negative change in its ability to execute, but rather a reflection of the broader enterprise DLP market evolution that changes the way we score vendors that do not offer all three primary channels.

Strengths

- It is differentiated by high-speed throughput and in-line network blocking.
- It has capabilities specific to using content-aware mechanisms to detect and address malicious code.
- It has strong internationalization, with multilanguage format support.
- Its Verdasys partnership for agent-based DLP and management console integration points rounds out the offering for clients willing to deploy both vendor solutions.
- It has a strong presence and continuing appeal for U.S. federal government/Department of Defense customers.

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 U.S. must go through partners for support.

GTB Technologies

GTB offers a balanced network, agent discovery and endpoint DLP portfolio, with a good price point for smaller organizations. While the product does not offer network discovery (only endpoint discovery at this time), it does support some innovative features such as a proprietary partial document matching capability. GTB is a small vendor focused on SMBs, such as credit unions.

Strengths

- GTB's policy definition and features for network functions are competitive with much larger vendors.
- Its good innovations in partial document matching algorithms offer a competitive means of addressing complex policy definitions.
- It has shifted its sales model to focusing on SMBs in financial services.

Cautions

- Its product suite does not offer network discovery.
- Although it has been in business for several years, GTB remains an early-stage company representing some vendor risk.
- Its endpoint DLP capabilities are limited to controlling data transfer to removable media, and it lacks self-remediation.
- Its interface is functional, but not as function rich or easy to use as many of the competitors.

McAfee

McAfee has successfully integrated its network, discovery and endpoint functions with common policy management through ePolicy Orchestrator (ePO), and competes effectively in the enterprise DLP market. It has also built an ecosystem of complementary functions such as endpoint disk encryption and device control, which strengthen the overall value proposition beyond pure enterprise DLP.

Strengths

- McAfee has worldwide presence, with a strong network of value-added resellers (VARs) that appeals to large, geographically distributed enterprises.
- It has 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.
- It has endpoint presence and network infrastructure, all managed with ePO, which has the potential to lower the cost of deployments for existing McAfee clients.

Cautions

- Its discovery file remediation is limited through the network discovery function, compared to remediation available through endpoint agent discovery.
- Its protocols over HTTP are not clearly identified in the user interface, adding some difficulty to addressing social-media use cases.
- The selection of McAfee DLP on the endpoint is typically preferred as a solution when the enterprise is also using McAfee for antivirus and other endpoint protection functions.

Palisade Systems

Palisade's PacketSure DLP offering has traditional content-aware DLP functions — including network DLP and endpoint discovery functions combined with URL filtering, IM proxy, application filtering and e-mail/Web proxy. It supports agent-based discovery capabilities at a very competitive, SMB-friendly price and packaging. Palisade sells primarily to SMBs across a variety of industries, including healthcare, financial services and education.

Strengths

- Its integrated appliance form factor with features typically needed by SMBs provides broad appeal in this market segment.
- It has partnerships with e-mail encryption solutions (PGP, Voltage Security and Cisco/IronPort) for automated remediation.
- Its new management oversight and investments have positively influenced product development and focused marketing resources on growing the company's SMB network-centric DLP offering.
- Its new traffic analysis (context and content) feature provides SMB network managers with valuable insight into sensitive communication flows.
- Gartner clients have reported on its ease of deployment and use.

Cautions

- While capability sets are expanding, Palisade's road map continues to follow the large-enterprise market, limiting the appeal of the solution to enterprises with less than 5,000 people and less-complex detection requirements.
- There are no network discovery or endpoint DLP functions.
- The masking of sensitive data from unauthorized users in the management interface is not supported.
- The market is quickly becoming crowded for low-complexity DLP deployments from channel DLP solution providers. This will require Palisade to aggressively expand its partner ecosystem.

RSA (EMC)

RSA (EMC) — also known as RSA, The Security Division of EMC — offers the RSA DLP Suite, which provides comprehensive network, discovery and endpoint enterprise DLP that addresses all the DLP elements required by customers across all industries. RSA (EMC) has licensed its DLP technology through OEM agreements with other large vendors, such as Cisco and Microsoft, creating an ecosystem of technologies integrated into its suite that provides alternate DLP delivery model choices to its customers.

Strengths

- Its strong described content capabilities are 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 appeals to geographically diverse clients.
- It has support for distributed discovery agents, with broad appeal for enterprises that wish to address complex discovery requirements across thousands of endpoints.

Cautions

- Its endpoint network functions are not supported in version 7.2, limiting its ability to address social-media use cases when endpoints are disconnected from the corporate network.

- Its ability to identify specific application protocols over HTTP.

- It is best-known for network and discovery content-aware DLP infrastructure solutions, with an endpoint offering that continues to be challenged by endpoint-centric and antivirus vendors — including those with channel DLP capabilities only.

Symantec

While Symantec Data Loss Prevention continues to be our highest-rated overall enterprise DLP capability, the gap has closed significantly during the past year. It provides comprehensive network, discovery and endpoint capabilities with excellent workflow.

Strengths

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

- It has support for double-byte characters and localized Windows OSs in 25 languages.

- Its integration with the new Data Insight product raises the bar in ability to extend content awareness into the enterprise to address the movement and use of sensitive data.

- Its new low-end offering, Symantec DLP Standard, targets organizations not requiring Symantec's traditional full-featured "enterprise-class" DLP. The offering supports an upgrade path when time/needs require it.

Cautions

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

- Gartner clients report operational and deployment complexities, indicating that organizations should budget resources appropriately.

- The selection of Symantec DLP on the endpoint is typically preferred as a solution when the enterprise is also using Symantec for antivirus and other endpoint protection functions.

Trend Micro

Trend Micro's LeakProof offers competitive endpoint capabilities, but continues to possess only below-average discovery capabilities and lacks competitive network functionality. It has launched an initial version of network DLP embedded in its Threat Discovery Appliance. Trend continues to play catch-up in the broader enterprise DLP market; however, it is appropriate for existing Trend Micro customers with endpoint-focused, basic DLP requirements, and SMBs considering low-complexity use cases.

Strengths

- Trend Micro has strong channel DLP endpoint capabilities.

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

- It has a proprietary partial document match hash algorithm, which yields improved efficiency over traditional "rolling" hash implementations.

Cautions

- Its average content-aware discovery capabilities and lack of a content-aware network appliance continue to limit Trend Micro's appeal in large accounts looking for a comprehensive enterprise DLP solution.

- Its workflow support is poor, lacking data masking for unauthorized users and appreciable case management.

Trustwave

Trustwave acquired Vericept on 26 August 2009. It offers a suite of enterprise DLP products with all the necessary components to address network, endpoint and discovery use cases. It offers DLP through perpetual or subscription licensing and also as a managed service. Vericept was in the Visionaries quadrant in 2009, based on a good product with limited ability to execute. Following the acquisition, the product line has moved to the Challengers quadrant based on significant improvement on ability to execute and new limitations in its DLP vision as part of the larger Trustwave business focused on helping organizations address Payment Card Industry (PCI) requirements.

Strengths

- It has strong network, discovery and endpoint DLP capabilities.

- It has support for its endpoint agent and discovery (SaaS) model.

- Its use of Content Analysis Description Language (CANDL) appeals to enterprises with unique and very specific content requirements.

Cautions

- It has minimal localization and double-byte character support, limiting its appeal for large enterprises and international markets.
- With the continued commoditization of endpoint DLP functions from established antivirus vendors, the Trustwave endpoint DLP agent will be challenged to compete in a market where basic DLP is a checkbox on an antivirus renewal.
- It is best-suited for organizations engaged with Trustwave for other software and services.

Verdasys

Verdasys' Digital Guardian offers a strong agent-based endpoint and server control product with content-aware functions. While the content-aware capabilities are not as strong as other products, Digital Guardian differentiates itself with strong audit and control features. Digital Guardian's suite of components provides an ecosystem for organizations that wish to control the entire data flow as part of a proactive protection of data on agent systems.

Strengths

- Its solution ecosystem is appealing to enterprises that require strong controls for the protection of sensitive information.
- It has good workflow and case management.
- It has the ability to audit every access and control the movement of files that contain sensitive data.
- It is the only vendor to support Linux on the endpoint.
- Its Fidelis partnership for network-appliance-based DLP and management console integration points rounds out the offering for clients willing to deploy both vendor solutions.

Cautions

- It has limited appeal outside large organizations requiring high-end control beyond traditional DLP requirements.
- It is very high priced for an endpoint-only solution, but the vendor has created a price structure to phase in capabilities at lower price points.
- Its limited network discovery functions through a new virtual appliance based on its endpoint technology.
- There have been continuing reports of scalability and platform challenges for some complex, diverse deployments, although the vendor has been addressing the issues.

Websense

Websense provides a comprehensive enterprise DLP capability through its Data Security Suite. It has all the components necessary to address network, endpoint and discovery use cases, offering customers a well-rounded content-aware DLP solution.

Strengths

- Websense has a global presence, with a diverse network of VARs, appealing to geographically distributed enterprises with a sweet spot of less than 5,000 seats.
- It leads with subscription pricing, but offers perpetual licensing for clients who require it.
- It has integration of DLP capabilities within the existing Websense Web Security Gateway, simplifying content-aware DLP deployments for current Websense customers upgrading to this product.

Cautions

- Despite Websense's good endpoint functionality, many organizations will choose to add endpoint DLP as a checkbox on their antivirus renewal with an incumbent antivirus vendor.
- Its case management is rudimentary compared to competitors.

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.