Gartner

Research

Publication Date: 10 August 2011 **ID Number: G00213871**

Magic Quadrant for Content-Aware Data Loss Prevention

Eric Ouellet, Rob McMillan

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

The market for content-aware DLP continues to grow at more than 20% year over year. Organizations seeking content-aware capabilities to address sensitive data have more options in 2011 than ever before, with three main categories of offerings being marketed by vendors:

- Enterprise DLP solutions (the focus of this Magic Quadrant), which provide organizations with advanced content-aware inspection capabilities and robust management consoles
- Channel DLP, which consists of content-aware DLP capabilities that are integrated within an existing application — typically email
- DLP-lite, a new subcategory of offerings that group a specific set of capabilities in a way that addresses a niche market typically by requirement, such as discovery only, or for a specific use case, such as small or midsize business (SMB), where a need may exist to monitor only a few protocols and provide a simplified management console or workflow

Commoditization Continues

The commoditization of endpoint products continues; however, the pace has slowed down dramatically during the past 12 months, resulting in more price robustness than previously witnessed. Specifically, endpoint solutions quickly went from $150 to $200 per endpoint to $50 to $80 per endpoint during the past few years. In the past 12 months, endpoint solutions have stabilized in the $35 to $60 range, depending on configuration options. The rise of content-aware functions in many traditional security and infrastructure products continues to increase its pace (see the DLP-lite channel comments above).

The integration of identity awareness in traditional DLP products is also continuing, however, at a less brisk pace. Email boundary security, secure Web gateways (SWGs) and endpoint protection platforms continue to be released by vendors with increased DLP capabilities. In many cases, the limited DLP feature set in these channel-specific solutions (C-DLP) or in DLP-lite offerings is sufficient to solve near-term business requirements for DLP — specifically when they relate to basic regulatory compliance requirements. Gartner projects that the majority of organizations (approximately 70%) may be able to deploy "good enough" DLP capabilities in evolving channel-specific or DLP-lite solutions by 2013 to satisfy government regulations with respect to private and sensitive data, and for the automated application of protection mechanisms, such as the encryption of email and the storage of sensitive content to USB and other removable storage media or portable devices.

There was no additional market consolidation in the past 12 months, with the exception of a significant investment by Blue Coat in Code Green Networks, resulting in a private-label OEM. The larger vendors that made acquisitions in past years were focused on integrating DLP features into more of the products in their portfolios in the hope of creating the "content-aware enterprise" — a state where an ever-expanding breadth of solutions deployed within an organization is capable of identifying content, understanding the context of its use and applying DLP rules. This results in a better security and regulatory posture, as well as overall increased awareness and risk profiling.

Large vendors were nearly always seen offering DLP as part of an enterprise product renewal, such as antivirus, SWGs and email hygiene. Many of the bids reviewed by Gartner offered extremely aggressive pricing incentives, especially when total deals reached into high six or seven figures. Although pricing overall has shown downward pressure, the average enterprise deal continues to range between $350,000 and $800,000, with 18% to 23% annual support (see

"Budgeting the Costs of Content-Aware DLP Solutions"). The four most quoted vendors by their competition were Symantec, McAfee, RSA and Websense.

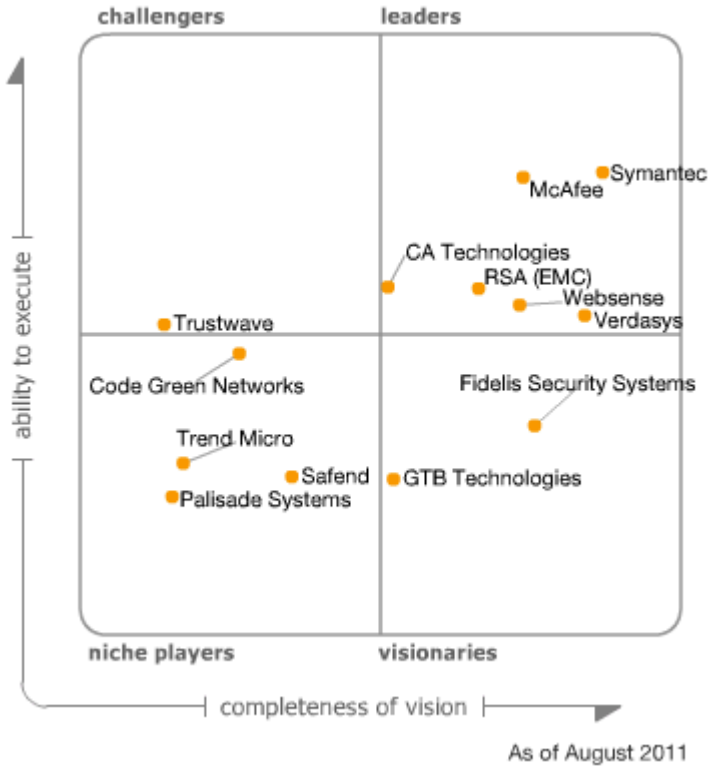
Content-Aware DLP Deployments Mature

As large and small organizations increase their deployments, DLP continues to mature and becomes better understood as a common control within the standard of due care. More organizations are now aware, more than ever, of what a realistic DLP deployment is and its associated time horizon for their enterprise requirements. Although Gartner continues to see organizations struggling with DLP deployments, more are willing to limit the scope of a DLP deployment and avoid "boil the ocean" thinking, resulting in more successful deployments as they obtain a better understanding of their DLP goals versus vendor product hype versus their internal constraints in terms of time, money, people and other resource requirements.

Although vendors continue to sell clients on the promise of what can be achieved by their most appealing and cool leading-edge features and capabilities (including described content data flows and ownerships, advanced/esoteric detection techniques and the integration of third-party remediation mechanisms), organizations need to focus their purchasing criteria on a clearly stated enterprise DLP strategy that addresses the fundamental question of, "What do we hope to achieve with a DLP deployment?" Although many organizations have an innate desire to have a fully content-aware corporate infrastructure that closely monitors the day-to-day use of sensitive data in all its forms, most organizations will rarely ever deploy more than the basic capabilities included in DLP offerings. As a result, Gartner has seen a significant increase in channel DLP and DLP-lite deployments in large and small organizations.

Lastly, it is imperative that organizations continue to be aware of the absolute need to involve non-IT/IT security stakeholders in the planning and operationalization of DLP. Although IT/IT security can play a role in ensuring the day-to-day operation of a DLP system, ultimately, the business needs to decide when an event is a policy violation and what the appropriate remedies for the incident are (see "Anticipate and Overcome the Seven Key Obstacles to Success in Content-Aware DLP Deployments").

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



Source: Gartner (August 2011)

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, email, packet, application or data store — while at rest (in storage), in use (during an operation) or in transit (across a network); and the ability to dynamically apply a policy — such as log, report, classify, relocate, tag and encrypt — and/or apply enterprise data rights management protections. DLP technologies help organizations develop, educate and enforce better business practices concerning the handling and transmission of sensitive data.

Content-Aware DLP Ought to Change Behavior

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 among vendors — in some cases, requiring custom integration with Microsoft Active Directory or other services.

Many vendors are experimenting with alternative delivery models, such as cloud, software as a service (SaaS) and more traditional managed service offerings for monitoring some types of network traffic (such as Web and email). No significant commercial offerings are available outside of Secure Email Gateway DLP integration, where DLP is used to identify sensitive content for redirection to an encryption service. 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.

Mobile Devices Pose a Challenge

Mobile devices have arrived and taken hold in the enterprise, resulting in many organizations struggling to establish appropriate terms of use — especially as they relate to the interaction with sensitive data. Although none of the DLP vendors represented in this Magic Quadrant offered integrated DLP solutions on the mobile device itself, several leverage the available "phone home" type of forced VPN tunneling from the mobile device to the corporate network, where traditional network-based DLP solutions can inspect the data intended to be disseminated from the device to an external entity. Lack of localized DLP capabilities on mobile devices is due in part to the variability of platform versions (Android, for example, has more than 250 variants of the OS designed for specific handsets/tablets, and not all capabilities are supported from one to another) and closed system architecture (iOS), although some vendors have implemented DLP solutions for tablets (specifically iPads). However, this lack of capabilities results in the risk of sensitive data loss by means of local storage on removable media, the transmission of data using alternate networking capabilities (Bluetooth as an example) and other avenues of loss or theft.

Virtualization, OS Support and Risk Reporting Are Still Lagging

The use of DLP for virtual environments was also reviewed and, at this time, remains a hit-or-miss capability for most vendors. Although some vendors supported the installation of a DLP agent on a virtual machine, few were able to scan a virtual disk file directly, resulting in increased effort required to perform data discovery within a virtualized environment.

Although many vendors have discussed plans to provide support outside of a traditional Windows platform (OS/X, Linux and Unix) during the next 12 months (something they also discussed in last year's Magic Quadrant), few vendors actually offered some capabilities. In fact, most of the plans discussed by vendors would result in severely capability constrained offerings on non-Windows platforms (for example, local data discovery only) that would barely support regulatory compliance requirements and would not include the advanced port control capabilities typically required for intellectual property (IP) deployments. The reality continues to be that, although these alternate platforms are considered top of mind share for clients because of a significant percentage of senior executive use and the growing wave of the consumerization of IT, they are not financially viable by themselves to the vendors. Until clients refuse to acquire solutions for lack of support of these alternate platforms, or hold back portions of payments until capabilities are delivered, most vendors will continue to suggest in perpetuity that "next year" will be the year they will finally offer support.

Gartner has seen client interest in the external certification of DLP products, including Common Criteria, the Federal Information Processing Standard (FIPS) and others. Currently, Fidelis, RSA and Safend have achieved Common Criteria certification. The process is well under way for

McAfee and Websense. CA Technologies plans to initiate this effort in 2011. FIPS 140-2 compliance has been achieved by McAfee, RSA, Safend, Symantec, Verdasys and Websense.

DLP business cases often include risk management as one of the cornerstone drivers, yet most, and arguably all, vendors do a poor job of representing risk in their reporting capabilities. Out-of-the-box reporting is typically based on the number and type of events that have been detected, which is a very DLP-oriented view. They do not take a risk-oriented view that looks at accumulated point-in-time risk linked to the type and value of the information asset that has been exposed or the value of the business process that has been compromised by the event. This requires a mind-set that goes beyond linking reports to the way in which the tool works to developing reports linked to the way in which they will be used outside the IT department.

Gartner Inquiry Data and Observations About Content-Aware DLP

Gartner inquiry data through 2011 indicates several major observations that should help organizations develop appropriate requirements and select the right technology for their needs:

- About 30% of enterprises led their content-aware DLP deployments with network requirements — 30% 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 of them 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 (see "Develop an Enterprise Strategy for Content Monitoring and Filtering/Data Loss Prevention," "Understanding the Value of Content-Aware DLP" and "2010 Content-Aware Data Loss Prevention FAQs").

- The primary appeal of endpoint technologies continues to be the protection of IP 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, in identifying and preventing accidental disclosures of sensitive data, and in providing a mechanism for supporting compliance and audit activities.

- DLP solution providers continue to focus on text-based data in their analysis of content. Although a few vendors are making inroads into identifying nontext data, such as images, video, audio and other media, these remain in the early stage. To advance capabilities, vendors will need to invest significantly in R&D during the next several years.

- Many DLP deployments are sold on the basis of being a tool to assist in risk management activities; however, most DLP solution reporting capabilities do not provide dashboard or feedback relevant for this function.

- Incumbent antivirus and endpoint protection vendors continue to lead clients' RFP shortlists.

The embedding of content-awareness functions in more products will enable the broad, effective application of protection and governance policies across the entire enterprise's 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 2014.

During the past year, the number of Gartner client inquiries regarding complaints about DLP vendor behavior has been on the rise. Many are characterized by an unpleasant trend within the industry where some vendor claims of supported capabilities are often provided with an unspoken caveat. For example:

- In the case of one vendor, the monitoring of a local CD/DVD writer was only supported when a third-party CD/DVD authoring software was installed. It was unable to monitor the built-in Windows-authoring client.
- In another case, the vendor claim of monitoring internal emails was only supported on a specific email platform.
- One large enterprise customer found that the capability of a major vendor's offering to detect unstructured data traversing the network has not met its needs, citing the complexity of the configuration and disappointing results for the detection of Web traffic.

As with all acquisitions, it is important to be clear with your shortlist of vendors of your planned deployment requirements and also the environment in which you expect the DLP functionality to be supported. Gartner recommends that organizations test the capabilities considered critical for a deployment before making a purchasing decision.

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 experienced steady growth. Content-aware DLP deployments and overall sales were only minimally affected by the economic downturn and rebounded in dramatic fashion throughout 2010 ($300 million) and 2011 ($425 million). Gartner estimates that this market will reach $520 million in 2012.

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 email communication
- Were generally available as of 31 January 2011
- 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, email, instant messaging and HTTP)
- Primarily support object tagging and then enforce policy based on the tags

Added

Safend was added to this year's Magic Quadrant.

Dropped

No vendors were dropped from this year's Magic Quadrant.

Evaluation Criteria

Ability to Execute

Our ratings are most influenced by four basic categories of capability: network performance, endpoint performance, discovery performance and management consoles. 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.

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 (August 2011)

Completeness of Vision

Content-aware DLP technologies are becoming more mainstream in North America, Europe and Asia. Large solution providers now offer DLP as 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 the Ability to Execute on that vision. Gartner continues to place 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 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 (August 2011)

Leaders

The Leaders quadrant has six vendors in 2011. The Leaders have demonstrated a good understanding of client needs and offer comprehensive capabilities in all three functional areas — network, discovery and endpoint — in addition to strong management interfaces 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 in development and address evolving market needs to remain in the Leaders quadrant. The Leaders are:

- CA Technologies
- McAfee
- RSA (EMC)
- Symantec
- Verdasys
- Websense

Challengers

Trustwave is in the Challengers quadrant again in 2011 based on the capabilities of its product and the challenges presented by a business model that continues to not focus on the DLP market. Its Ability to Execute remains somewhat unchanged from 2010, but its lack of DLP product enhancements has resulted in a slip in vision positioning. 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 — GTB Technologies and Fidelis Security Systems — have very different backgrounds in this market. GTB has primarily focused its efforts on developing a product with strong detection capabilities, and continues to improve the overall user experience. It has also achieved notable client wins in the past 12 months, thereby increasing its

overall market presence. Fidelis continues to innovate and lead the network DLP appliance sector and now incorporates significant add-on capabilities that can help identify potential risks before they occur.

Niche Players

The Niche Players quadrant has four vendors for 2011:

- Code Green Networks' product expansion during the past year into the enterprise market has received a somewhat lukewarm reception. Capabilities that were lacking in previous years that remain to be fully addressed have resulted in a lower Completeness of Vision ranking.
- Palisade Systems continues to focus on capabilities that are focused on the low-deployment-complexity end of the SMB market. Although client satisfaction remains high, management changes and other issues during the past 12 months seem to have impacted its overall responsiveness and growth.
- Safend is a new entrant in the 2011 content-aware DLP Magic Quadrant. Its capabilities and integration were at a sophisticated level, given the overall maturity of this market.
- Trend Micro's DLP offering continues to lack critical capabilities and integration, resulting in an offering that is significantly lagging the capabilities of competitors' products. Trend Micro's continued focus on selling primarily to its existing antivirus client base is resulting in sales levels that are lackluster compared with the competition.

Vendor Strengths and Cautions

CA Technologies

In the past 12 months, CA Technologies addressed many capability shortfalls of previous releases, including content detection functions. It also leveraged integration with other CA Technologies offerings, resulting in broader deployments. These and several factors discussed below resulted in the position change to the Leaders quadrant.

Strengths

- CA Technologies continues to have a forward-looking vision, including the integration of content-aware DLP capabilities with its log management and identity and access management (IAM) offerings.
- CA Technologies has a proven competency in delivering content-aware DLP capabilities for isolating sensitive content within different regulatory compliance domains. It has formalized this and its broader deployment capabilities in its Rapid Implementation Services Offering (RISO).
- It is scalable and has a proven capability for securing messaging infrastructures.
- CA Technologies has strong workflow and event management, with DLP support for social media use cases common in many enterprise deployments.
- It has a good overall blend of available preconfigured policies that cater well to its primary customer base of North American financials.

- CA Technologies has global reach, appealing to large, geographically diverse enterprises. End-user interactions for the endpoint, network and stored data capabilities are localized.

Cautions

- CA Technologies still lacks advanced native content search capabilities. It plans to address some of these by integrating Autonomy's Intelligent Data Operating Layer (IDOL) components in future releases. Database content registration is still not supported.
- CA Technologies' management console is very functional and feature rich; however, it is fragmented with different interfaces, and has a severely dated look and feel. It would benefit from a significant refresh. It currently supports English only.
- Although CA Technologies continues to push its IAM/DLP vision, it continues to be in a perpetual catch-up mode when compared with other offerings. Deployments using these capabilities in production environments continue to lack maturity.

Code Green Networks

The formalized relationship with Blue Coat Systems (via a significant investment) and partnerships such as with Palo Alto and others are bringing in increased visibility and sales from a larger enterprise market. Its proven strength remains in easy-to-use, low-cost, content-aware network DLP. Although it has invested in expanding some of its core capabilities, the level of effort and progress is resulting in an offering that is not advancing as quickly as its peers. As a result, it has moved firmly into the Niche Players quadrant from the Visionaries position it held for many years.

Strengths

- Code Green Networks' product is aggressively priced and has a comprehensive list of starter policies.
- It has good baseline network capabilities, with a primary focus on ease of deployment and use. It has a proven track record with smaller businesses (fewer than 2,500 users) and is expanding is footprint into 5,000-user and larger organizations.
- Code Green Networks' good Active Directory integration simplifies deployment and workflow.
- Its embedded message transfer agent (MTA) functionality and flexible native email encryption capabilities — via the integration of ZixCorp and Cisco/IronPort systems' secure envelope and Voltage Security Network (VSN) technology within the product — add significant value for SMBs, which typically prefer integrated solutions.
- It supports double-byte characters, and the management console can be localized using language settings on the viewer's desktop.

Cautions

- Code Green Networks' endpoint agent has been enhanced; however, it continues to be missing key capabilities when compared with other vendors.

- Its discovery capabilities with local agent software relies on a "phone home" capability to the network appliance for advanced detection that is unavailable when offline or off-site. Generalized discovery scans rely on a spreadsheet for configuration details.
- Integration with SIEM is only supported via Syslog and automated email.
- DLP policies are not always consistent among endpoint, discovery and network.
- Social media and mobile device DLP support are planned only for future releases.
- Deployments outside the U.S. are managed primarily through a patchwork of strategic local partners that are supplemented by Code Green Networks' staff.

Fidelis Security Systems

Fidelis Security Systems' XPS product line offers innovative and market-leading network content-aware DLP capabilities. Support for non-DLP capabilities (threat intelligence feeds, intelligent network forensics and user awareness) identifies potential threats and risks in a large diversified environment. Its product supports strong SIEM integration. Fidelis does not offer endpoint capabilities and has very limited network-centric discovery capabilities. These capabilities are provided via a partnership with Verdasys.

Fidelis offers a strong and highly scalable content-aware network DLP product that addresses the needs of large enterprises looking for network-only capabilities. Fidelis' move into the Visionaries quadrant from the Niche Players quadrant is a recognition that its core appliance offering is market-leading.

Strengths

- Fidelis 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.
- Fidelis' dashboard is very comprehensive, with advanced event search capabilities. It has strong workflow with good separation of duties via role-based access control (RBAC).
- It has strong internationalization, with multilanguage format support.
- It has a strong presence and continuing appeal for U.S. federal government/Department of Defense (DoD) customers.

Cautions

- Its stated intention to offer only network DLP reduces the company's appeal to organizations looking for comprehensive enterprise DLP capabilities.
- The Verdasys partnership is required to round out the offering (endpoint and discovery) for clients willing to deploy both vendors' solutions.
- Fidelis' best-of-breed functions are appropriate for U.S. government/DoD 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 Technologies offers a technically focused product with network, endpoint and some discovery DLP capabilities. It is offered at a very attractive price point and supports some innovative features, such as a proprietary partial document matching capability. GTB is expanding its client base beyond SMBs, such as credit unions, with a new focus on developing technologies to address IP requirements and nontraditional DLP data, such as voice and video. GTB is one of the few vendors that offer access to its technology via a software development kit program.

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 is introducing innovative DLP features that go beyond traditional DLP content analysis. GTB's DLP solution can be deployed as an appliance or a virtual machine that can simplify deployments in smaller organizations.

Cautions

- Although network and agent discovery features are present as part of this release, performance needs to increase to support large unstructured environments.
- GTB was slow compared with other vendors to release 64-bit versions of its client agent solution.
- It does not support the input of a justification for events that end users want to proceed with as is.

McAfee

McAfee provides a very mature DLP offering that supports network, discovery and endpoint features that are integrated through ePolicy Orchestrator (ePO). McAfee is broadening its traditional client base to include new customers to McAfee and also nonfinancial organizations that are focused on IP protection. McAfee continues to expand its ecosystem of complementary functions, which strengthen the overall value proposition beyond pure enterprise DLP.

Strengths

- McAfee has a worldwide presence, with a strong network of value-added resellers (VARs) that appeal to large, geographically distributed enterprises.
- It has strong value for current enterprise users of McAfee's other endpoint solutions (for example, antivirus tools).
- Its ability to create a large database of day-to-day user/data interactions that can be used to "back test" new policies is unique in this market and can significantly facilitate in the reduction of false positives.
- McAfee has strong social media (such as Facebook) DLP enforcement capabilities.
- Its updated management console redesign and integration facilitate use; however, some common tasks still require multiple clicks.

- Its enhanced and simplified ePO integration has the potential to lower the cost of deployments for existing McAfee clients.

Cautions

- McAfee does not support admin interface localization, which can be important for large geographically dispersed organizations.
- The selection of McAfee DLP on the endpoint continues to be preferred as a solution when the enterprise is also using McAfee for antivirus and other endpoint protection functions.
- McAfee client references and Gartner client inquiries have not been universally glowing. Reports of inconsistencies in technical support and capabilities are distractions that need to be addressed by the organization before they take hold.

Palisade Systems

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

Strengths

- Palisade's integrated appliance form factor with features typically needed by SMBs provides broad appeal in this market segment.
- It has partnerships with email encryption solutions (for example, PGP, Voltage Security and Cisco/IronPort) for automated remediation.
- Gartner clients have reported on its ease of deployment and use.

Cautions

- While capability sets are expanding, Palisade's road map continues to follow a slow pace of evolution when compared with other vendors. The solution in its current form is clearly focused on small organizations with a low level of complexity in their detection requirements and use cases.
- The endpoint agent does not support the DLP monitoring of local network activities.
- 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 and DLP-lite solution providers. At the current pace, these providers will overtake Palisade in terms of capabilities within the next 12 to 18 months.
- Palisade's latest management changes (the third in four years) put into question the overall direction and focus of the organization. Although existing clients did not report being overly affected during the latest transition phase, this lack of consistency is a distraction that would best be resolved.

RSA (EMC)

RSA — 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. Although RSA has licensed its DLP technology through OEM agreements with other large vendors, such as Cisco and Microsoft, this has provided limited benefits for RSA. Plans to support additional integration partners have yet to materialize. Integration of DLP capabilities with other RSA and EMC products, including enVision and VMware, is starting to yield results. Although OEM sales are getting good traction, overall enterprise deployment growth has been steady, but does not appear to be keeping pace with other leading vendors in this market.

Strengths

- RSA's described content capabilities are good. They 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 and DLP support of data in many languages appeal to geographically diverse clients.
- It supports distributed discovery agents, with broad appeal for enterprises that want to address complex discovery requirements across thousands of system endpoints.
- Its innovative severity-ranking capability provides valuable context when leveraged by an experienced operator.
- RSA has very strong support and advanced features for the deployment of DLP to monitor virtual environments.

Cautions

- The endpoint agent continues to be weak in critical network functions, such as email, Web mail and social media support. In addition, Gartner clients have reported a growing number of issues during the past 12 months with the endpoint.
- The administration console is not localized in any language other than English.
- RSA 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 and DLP-lite capabilities only.
- Although RSA's management console is very functional, it could use an update to minimize the amount of scrolling and clicking required to view or perform a task. This additional level of work can become a source of frustration for everyday system users.

Safend

Safend is the first new vendor in the DLP Magic Quadrant in several years. Its Data Protection Suite is a DLP agent-based solution that has appeal for simpler DLP use cases that are primarily focused on regulatory compliance. Integration with other Safend products offers a simple upgrade option to existing clients.

Strengths

- Safend is a good solution for SMBs looking for a simple-to-use DLP solution to address typical regulatory compliance use cases.
- Integrated encryption capabilities ensure that sensitive files are protected when copied to mobile media and devices.
- The Mac OS/X client supports local discovery of sensitive information.
- Safend has good localization of the desktop agent. Its management console is localized in English, German and Japanese.
- Logs and event data are encrypted and digitally signed.

Cautions

- Safend offers an agent software solution only. No stand-alone network DLP solution is provided. Network discovery is accomplished via an endpoint agent.
- It does not provide an integrated event or case management solution.
- Although social media (for example, Facebook, LinkedIn and Twitter) are addressed, capabilities are limited.
- Pricing is higher than would be expected for a solution with these capabilities.

Symantec

Symantec Data Loss Prevention is the highest-rated enterprise DLP solution in terms of vision and execution in 2011 because of its breadth and depth of capabilities. Although other vendor solutions are providing significant competition, Symantec continues to be listed by competitors as the top vendor they encounter in RFPs. Symantec provides comprehensive network, discovery and endpoint capabilities with a well-integrated workflow that appeals to large, complex environments.

Strengths

- Symantec has a global presence, with a strong VAR network that will appeal to large, geographically distributed enterprises.
- It has good social media support.
- It has strong internationalization support. The management console is localized in eight languages, and the agent is localized in more than 25 languages.
- The integration of DLP capabilities or data flows with other Symantec offerings is considered a key determining factor by clients.
- Symantec's mature and well-supported deployment methodology provides clients with a good planning guide and support for their deployments.
- Integration of DLP capabilities within other Symantec offerings is creating a framework for the "content-aware enterprise."
- The continued execution of its strong vision positions clients with a solid upgrade path in years to come.

Cautions

- Symantec continues to have the most expensive full-suite enterprise license costs of any vendor and is commonly seen by clients as inflexible with its pricing.
- Gartner clients continue to report operational and deployment complexities with deployments because of the underlying architecture. Although typical large Symantec clients are generally capable of dealing with these issues, they do stress the need to budget project funding and staffing resources appropriately.
- Gartner clients and references continue to report that Symantec's sales organization is unaccommodating or inflexible during the sales process.

Trend Micro

Trend Micro's endpoint and network DLP products offer capabilities at an attractive price point for SMBs, but the slowing of feature upgrades is raising questions about its level of dedication overall to DLP as a business. Trend Micro is losing its catch-up battle in the broader enterprise DLP market. The solution is best suited for existing Trend Micro customers that have an endpoint focus with basic DLP requirements, and SMBs considering low-complexity use cases.

Strengths

- Trend Micro has a global presence, with a strong network of VARs that will appeal to geographically distributed SMBs.
- Endpoint DLP continues to address SMBs' low-complexity deployments well with a good baseline set of capabilities.
- Trend Micro has good interaction of DLP and USB device control use cases.
- Its improved management console provides event and trending data reporting and dashboards.

Cautions

- Although other vendors in this market continue to innovate and introduce new features, Trend Micro products continue to lack critical capabilities to support discovery and advanced network DLP that are considered the baseline for other offerings. Many future road map items are several releases behind what is competitively available today. For example, Windows 7 64-bit endpoint support was not available at the time of publication, and network DLP still supports only monitor and report capabilities. SIEM integration is not available even via Syslog.
- Trend Micro's solution is unable to resolve the IP address to machine name or user when a policy violation occurs.
- Workflow support continues to be poor, lacking data masking, RBAC and case management.

Trustwave

Trustwave 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. The ongoing product vision continues to

be narrowly focused on helping organizations address Payment Card Industry (PCI) requirements.

Strengths

- It has good network, discovery and endpoint DLP capabilities; however, client focus throughout the past few years has been on PCI compliance deployments.
- Trustwave has good reporting capabilities and dashboards that can integrate with SIEM solutions. All records captured by the system are encrypted and signed.
- It offers flexible licensing options, including perpetual, subscription and SaaS, with pricing terms that appeal to the budget-conscious.
- Trustwave's solution is capable of scanning individual VMware files (for example, .vmdk files) for sensitive data.

Cautions

- Minimal client localization (English and Spanish), a management user interface that is only in English and the lack of double-byte character support limit Trustwave's viability in large enterprises and international markets.
- Its product does not support justification for event notification.
- Lack of investment in product feature enhancement is limiting Trustwave's appeal beyond the SMB market.

Verdasys

Verdasys' Digital Guardian offers strong agent-based endpoint and server agent DLP solutions. With the formalization of an OEM agreement with Fidelis and the integration of management console capabilities, Verdasys now provides a full suite of DLP capabilities directly to its clients, which has resulted in its placement in the Leaders quadrant. Digital Guardian differentiates itself with strong audit and control features. Digital Guardian's suite of components provides an ecosystem for organizations that want to control the entire data flow as part of a proactive protection of data on agent systems. This capability is strongly regarded by clients deploying DLP to address IP protection requirements.

Strengths

- Verdasys' solution ecosystem is appealing to enterprises that require strong controls for the protection of sensitive information.
- It offers strong workflow and case management with a simple and easy-to-use process for creating custom dashboards and reports.
- It has the ability to audit every access to (and control the movement of) files that contain sensitive data, which is a capability sought after by IP firms and organizations fearing WikiLeaks-type data disclosures.
- Verdasys supports Linux on the endpoint.
- Its integrated encryption capabilities ensure that sensitive files are protected when copied to mobile media and devices.

- The ability for the Verdasys management console to manage Fidelis' network appliance and events greatly streamlines deployment of both solutions and enhances the value proposition of deploying both solutions.

Cautions

- Lack of a simplified channel or DLP-lite offering means that Verdasys has limited appeal outside large organizations that require high-end control beyond traditional DLP requirements.
- Its pricing continues to be at the premium end of the market. Its pricing structure supports a phased deployment of capabilities at lower price points.
- Limited RBAC with a lack of federated delegation in the console continues to be a weakness that concerns some customers and prospects.
- Verdasys' solution and capabilities can be viewed as complex because of its level of flexibility for some deployments, and require appropriate planning and resource allocation to obtain best results.

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. Websense has a global presence and a diverse network of VARs, which is appealing to geographically distributed enterprises with a sweet spot of less than 5,000 seats.

Strengths

- Websense offers a good overall solution, with equally strong DLP capabilities in endpoint, network and discovery.
- It leads with subscription pricing, but offers perpetual licensing for clients that require it.
- It offers DLP as SaaS.
- A Linux endpoint agent is available.
- Websense's strong endpoint and user alert localization will appeal to global organizations.
- Its unique approach with the Triton platform simplifies deployments and the acquisition of Websense solutions requiring only entering a new license on the centralized appliance.

Cautions

- Websense offers a very capable and comprehensive management console that is easy to use and provides strong reporting and charting capabilities; however, it is only in English.
- Although deployment growth has accelerated in the past year, Websense needs to continue to enhance its VAR support initiatives to ensure global presence and expertise availability.

RECOMMENDED READING

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Anticipate and Overcome the Seven Key Obstacles to Success in Content-Aware DLP Deployments"

"Roundup of Content-Aware DLP Research, 3Q10"

"Budgeting the Costs of Content-Aware DLP Solutions"

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 competes in/serves 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 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 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 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), the availability of user groups and service-level agreements.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, such as 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: The 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 website, 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 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 vertical industries.

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 — directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner