Magic Quadrant for Content-Aware Data Loss Prevention

3 January 2013 ID:G00224160

Analyst(s): Eric Ouellet

VIEW SUMMARY

As the enterprise content-aware DLP market evolves, vendors are integrating adjacent technologies to create a broader ecosystem of DLP-enabled solutions. Channel DLP and DLP-lite offerings are gaining client mind share and focusing on low-complexity regulatory compliance use cases.

Market Definition/Description

Gartner defines content-aware data loss prevention (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.

Content-aware DLP technologies can be generally divided into three separate categories:

Enterprise content-aware DLP solutions incorporate sophisticated detection techniques to help organizations address their most critical data protection requirements. Solutions are packaged in agent software for desktops and servers, physical and virtual appliances for monitoring networks, and agents and soft appliances for data discovery. One of the leading characteristics of enterprise content-aware DLP solutions involves a centralized management console, support for advanced policy definition and event management workflow.

DLP-lite products typically use fewer and less sophisticated detection techniques, and they support only a limited number of protocols (for example, email, Web and FTP). Deployments tend to be exclusively endpoint or network, or for data discovery only. Solutions typically have limited consoles supporting basic centralized policies and very limited event management — if included at all.

Channel DLP is a limited content-aware DLP feature set that is integrated within another product — typically email encryption. Channel DLP in this mode is used to facilitate the end-user decision process to questions such as "Should I encrypt this email?" by doing the analysis for the user and automatically determining whether encryption is applicable or required. Channel-DLP technologies are usually focused on a limited set of primary use cases, mainly regulatory compliance. See "Guidelines for Selecting Content-Aware DLP Deployment Options: Enterprise, Channel or Lite" for a more detailed discussion.

The enterprise content-aware DLP market has experienced steady growth during the past seven years, with content-aware DLP deployments growing from 2010 ($300 million) to 2011 ($425 million) to 2012 ($535 million). Gartner estimates that this market will reach $670 million in 2013.

Return to Top

Magic Quadrant

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

STRATEGIC PLANNING ASSUMPTIONS

Content-aware DLP will be part of the standard of due care by 2013 in North America, and by 2015 in Europe and the Asia/Pacific region.

By 2014, more than 50% of enterprises will use some form of content-aware DLP capability, but only 30% of them will have a comprehensive enterprise content-aware DLP solution or strategy.

EVIDENCE

This Magic Quadrant was developed using Gartner's well-defined methodology. This process incorporated the following to gather primary data about each vendor's offering:

A categorization survey gathered a high-level view about which vendors should be included and excluded from the Magic Quadrant.

A full survey was used to collect detailed information about the vendor and its offerings.

Demos were conducted to view the offering in action, and verify elements in the survey responses.

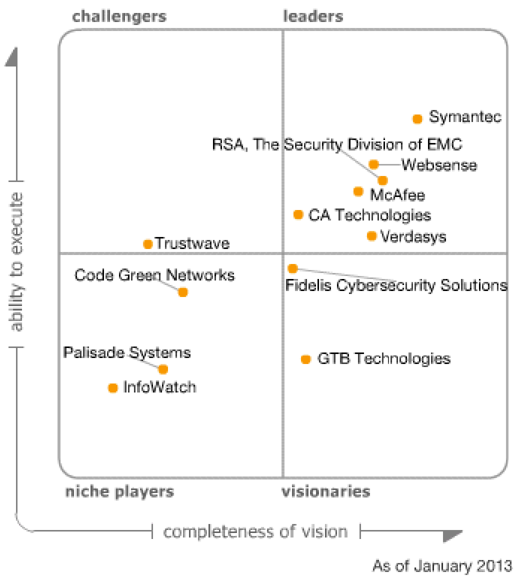
References were contacted to gather information about the customer experience, verify elements in the survey responses and identify any other elements of interest beyond those covered in the survey.

Guidelines for responding to the full survey were provided at the time of issue of the survey. Responses were of variable quality.

Responses that were lower quality (for example, ignored the question, poor grammar, inability to explain key concepts, inability to provide high-quality explanations of use cases, and inability to go beyond technical capabilities and demonstrate an understanding of the business environment) or did not meet the guidelines generally tended to score lower. One vendor declined to provide a survey response or participate in any other way. Some vendors declined to answer certain questions because of market restrictions and, therefore, did not fare as well under some of the scoring criteria.

Demonstrations were critical, because they illustrated points that are difficult to make in writing, and provided an opportunity to illustrate features not otherwise covered in the survey. All survey respondents provided a product demonstration using a formal script provided by Gartner. Demonstrations were terminated after a set period of time, regardless of whether the entire script had been completed. The demonstration scripts were intended to be difficult, but possible, to complete within the time period in order to force a focus on the key aspects with few irrelevant distractions, and also to demonstrate whether the product was easy to work with. Demonstration quality varied, ranging from very poor to outstanding.

We asked for five references from each vendor, and each reference customer was supplied with a structured survey. References were scored on the basis of the quality of the reference and what the reference told us. For each vendor, we take into account comments from that vendor's own references, and what



Source: Gartner (January 2013)

Return to Top

Vendor Strengths and Cautions

CA Technologies

CA Technologies continues to have a solid offering but struggles to articulate its value proposition clearly outside of its core market of clients. CA DataMinder now incorporates universal indexed searching using Autonomy's Intelligent Data Operating Layer, addressing one of the cautions from last year's Magic Quadrant. CA Technologies is looking to build its market share by developing new offerings targeted toward deployments outside the U.S. and also for new technologies, such as cloud services (for example, through the DLP-as-a-service offering).

Strengths

CA Technologies' focus on the relationship between identity management and DLP is among the strongest.

Support for messaging infrastructures remains a strong value point, and CA Technologies has a loyal customer base in the financial sectors.

Support this year for fingerprinting/data registration is a welcomed addition to a comprehensive and globally localized rich product feature set and policy language.

Clients continue to report that CA Technologies' global sales and support are strong buying criteria.

Cautions

Customers comment that CA Technologies' policy and event management function is not as intuitive or as easy to use as that of competitors with similar capability sets. Although all the components required to support comprehensive event management and workflow are present in the offering, the interface lacks finesse and clarity, resulting in an offering that appears less than full-featured.

Although its policy language is comprehensive, it is minimally documented, which results in added complexity in policy definition and tuning time for advanced deployment scenarios.

CA Technologies' interface, which was a weak point last year, has improved in the past year and reflects some of the common client feedback; however, it is still considered by Gartner to be dated in design, and clients continue to report that it is difficult to use.

Return to Top

Code Green Networks

Code Green Networks continues to lag behind in the growth and evolution of its product offering, as compared with other vendors reviewed in this Magic Quadrant. Although Code Green has initiated investments into creating an enterprise-grade version of its offering during the past several years, its overall DLP product continues to be primarily geared to small and midsize deployments with low complexity use cases.

Code Green's channel relationship with Blue Coat Systems is expanding into a technology integration with Blue Coat products, in which Code Green's offering will have a supporting role in a channel-DLP deployment context. This channel-DLP approach seems to be emerging as a more consistent theme overall in the way Code Green perceives itself and its value to clients.

Strengths

other vendors' customers said about that particular vendor. For example, when scoring Symantec, we took into account what Symantec's own customers said, as well as what the customers of other vendors said about their experiences with Symantec — if they had any. Scores for each vendor were normalized. If we receive fewer than three references for a vendor, we scored missing references as a "0." Vendors can be notably affected by the inability to have sufficient reference customers provide input.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): 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, SLAs 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 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.

Code Green improved its endpoint capability in 2012 to support autonomous local data discovery scanning, without requiring a connection to an available network appliance to conduct the actual content analysis.

Code Green's simple-to-use interface and workflow for USB control facilitate the triggering of user actions and justifications when copying content to USB.

Its solution supports a native data encryption capability.

Cautions

Minimal addition of advanced DLP capabilities or integration with related risk compliance, identity and access management, or enterprise digital rights management/information rights management solutions is resulting in a basic DLP offering that supports only the core needs of a primarily U.S.-focused regulatory compliance client base.

Although Code Green previously had yielded strong capabilities in DLP for international deployments, lack of continued investment has all but stalled deployments beyond Japan and India.

Code Green's offering is best-suited for small and midsize deployments with low-complexity use cases due to weak reporting capabilities and task-heavy quarantine functions, which can necessitate manual administrative intervention for each event.

Return to Top

Fidelis Cybersecurity Solutions

Fidelis Security Systems was acquired by General Dynamics in August 2012 (see "General Dynamics Deal Will Accelerate Evolution of Fidelis' Market Focus") and renamed Fidelis Cybersecurity Solutions. This is the only acquisition reported in the content-aware DLP market in over two years. Fidelis will continue to operate as a stand-alone company under General Dynamics and has integrated General Dynamics' security consulting organization as part of its team of consultants.

Fidelis continues to offer one of the strongest and highest-throughput network DLP capabilities available in the market today. Clients report using Fidelis' content-aware DLP offering to protect against information loss from network communications going outside their enterprise and from targeted externally sourced threats. Fidelis has been investing significantly in enhancing its advanced persistent threat-management-like capabilities to expand its role in protecting against external threats.

Fidelis has an OEM partnership with Verdasys, where Verdasys offers integrated Fidelis DLP and cyberthreat defense capabilities within its management console. General Dynamics, Fidelis and Verdasys have all stated publicly and to Gartner their joint intent to continue this relationship. Although there are always risks associated with acquisitions of this nature, it is Gartner's belief that the existing relationship will continue as is for at least the next 12 months.

Strengths

Fidelis has one of the strongest content inspection and network throughput capabilities available in a content-aware DLP appliance.

Its differentiating approach emphasizes protecting from external threat sources, in addition to traditional internally sourced DLP.

Its product road map provides evidence of strong vendor responsiveness and a process that enables customers to influence product direction.

Fidelis' malware protection capabilities are a differentiator.

Cautions

The Fidelis offering can easily support simple DLP regulatory compliance deployment use cases; however, there are lower-cost and simpler alternatives available in the market.

Although the product provides industry-leading content detection and event analysis, workflow and other administrative functions are more basic in comparison with enterprise content-aware DLP vendors.

Event severity is not granular and does not take into account event details to the extent that some other offerings do.

Although General Dynamics has announced that the relationship between Fidelis and Verdasys — along with the current DLP road map — will not change, existing customers should understand that there are always inherent risks during a change of ownership.

Return to Top

GTB Technologies

GTB Technologies provides a complete content-aware DLP solution set that offers capabilities to support both regulatory compliance and intellectual property (IP) use cases using endpoint, network and discovery. Most deployments are within small or midsize businesses (SMBs) that rely on a relatively small team of administrators to support their users.

Strengths

Clients report that GTB is very responsive and adaptive to their deployment needs.

GTB is among a very small set of content-aware DLP vendors that have integrated enterprise

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.

digital rights management/information rights management remediation capabilities directly within their DLP solutions.

GTB's investment in enhancements to their UI has resulted in improved ease of use when deploying policies across any combination of network, endpoint or discovery.

The vendor is focusing on making the solution cloud-ready.

GTB's content-aware DLP capabilities for a virtualized environment were highly rated by clients.

Cautions

GTB's products are focused on technical capabilities, rather than workflow and providing simplified means of addressing business concerns over data loss. Although this approach has its merit with smaller organizations, larger deployments must emphasize the business unit's role in content-aware DLP deployments, which can be more difficult to realize with the existing offering.

Although GTB made significant improvements in its UI, Gartner assesses that the overall solution maintains an inconsistent look and feel across the various product components.

Gartner assesses that the reporting and audit logging are basic when compared to competitors selling to large enterprises. The solution only provides access to events, rather than providing a relationship with risk-based reporting.

Return to Top

InfoWatch

InfoWatch is a Russian-based content-aware DLP vendor that has sold solutions in Russia since 2004. InfoWatch began its international sales expansion during the past year, and is showing good product capability development, innovative features and a relative high level of maturity for a new product. Although it is not quite ready to be called enterprise-grade, it provides significantly more capabilities than most DLP-lite offerings in the market.

InfoWatch has established an early track record of happy customer references, which included typical content-aware DLP adopters in the banking sector, but also included entertainment and media organizations, which is not as typical. As would be expected, InfoWatch's customer base was primarily located outside of North America, but efforts are being put into place to support sales expansion via partners and resellers.

Strengths

InfoWatch offers strong language and internationalization support.

It supports USB device monitoring.

Its color-coding of event type and severity is innovative.

Sensitive data substitution is supported using shadow copies of files. The original is retained, yet the sensitive content is removed before it hits the presentation layer.

Cautions

Although its overall offering demonstrates promise, it is still in an early stage, with basic network and endpoint capabilities and no current support for data discovery.

InfoWatch's product does not have built-in policies. It provides industry-specific content filtering databases, which clients can either use to create their own policies or engage with the vendor to build policies on their behalf.

Its console and policy engine are basic. Content inspection and detection are limited and do not include advanced detection mechanisms. InfoWatch uses a multistep scripting process using a flat file containing policy definitions. The process requires contacting vendor support to create new policies. This can result in severe client dissatisfaction over the disclosure of the nature of the content-aware DLP inspection clients want to perform.

Logging relies on Oracle Database and is not natively integrated.

Return to Top

McAfee

Now part of Intel, the McAfee content-aware DLP solution has undergone significant improvements since the publishing of the previous content-aware DLP Magic Quadrant. Although the overall offering does not possess some of the impressive niche use-case features provided by some of its competition, several of the standard features included within the product offering are better than its competitors.

The key differentiator, outside of the McAfee ePolicy Orchestrator (ePO) integration, remains the capture database. This centralized inventory of activity data is used in the testing and streamlining of new policies to address possible false positives and to reduce deployment time.

Customer satisfaction was an issue in previous Magic Quadrants for McAfee, and the vendor continues to score relatively low in this area. Clients also reported concerns over long-term product innovation under Intel's ownership of McAfee. At the end of 2011, there was a significant reduction in the overall size of the content-aware DLP team because of internal realignment. This is in sharp contrast with other vendors in this market that made and continue to make significant investments in their core team and adjacent product head count. Although this situation has been corrected during 2012, and the dedicated staff count has increased, it continues to be significantly below the levels of other vendors in the Leaders quadrant.

Strengths

McAfee's case management workflow is one of the strongest in this market, and enables both comments and extra documents to be added or deleted from the case record as required in the different stages of event management.

Detection on nontext content (for example, pictures) is based on both the content and metadata.

Its endpoint DLP product can be deployed in a stand-alone configuration.

Features geared toward emerging platforms, such as social media and mobile devices, were notably good.

The capture database, which allows for previously captured data to be used for analysis and testing new rules, is an innovative and distinctive feature that has been well-received by clients and continues to be reported as a leading feature for clients adopting the McAfee content-aware DLP solution.

Cautions

The redaction function either encrypts sensitive content (network) or replaces files with placeholders (endpoint). It does not maintain the integrity of the content, because it simply replaces the sensitive portion with substituted text.

McAfee continues to have a basic offering for virtualized environments. Although Gartner observes that the technology is used in virtualized environments by some customers on an experimental basis, it was not officially supported by McAfee at the time of this analysis. McAfee's approach to virtualization is not as well-articulated as some of its competitors.

Customers have expressed to Gartner some frustration with McAfee's support for the management of incidents —in terms of both capacity and organizational capabilities.

A variety of minor issues reported by clients suggests room for improvement in quality assurance, including reports that updates, for example, have on occasion broken existing features, and that product documentation is not to the standard of its peer competitors because of outdated or incomplete content.

Return to Top

Palisade Systems

Palisade Systems' PacketSure DLP offering has had only minor capability enhancements in the past year. Product capabilities remain firmly within the traditional regulatory compliance segment of content-aware DLP deployments. The offering supports network, endpoint and agent-based discovery functions. The PacketSure DLP appliance solution combines URL filtering, IM proxy, application filtering and email/Web proxy in a single offering at an SMB-friendly price. Leading customer deployments include presence in the healthcare, financial services and education sectors.

Strengths

Simplicity of deployment and integration with Web and mail security services remains a high note for Palisade clients.

Palisade provides a reasonably comprehensive list of default policies that is directly applicable in a regulatory compliance deployment use case.

Palisade supports email encryption solutions (for example, Pretty Good Privacy, Voltage Security and Cisco-IronPort) for automated remediation.

Although the Palisade offering is not as technically sophisticated as that of other vendors, customers tend to be very happy with their deployments.

Cautions

Although the product is competitive within the SMB space, lack of significant investment in the development of more advanced capabilities and more streamlined management results in a product that has limited appeal beyond low-complexity SMB deployments.

Gartner assesses that the management interface is not as intuitive or as easy to use as it could be for the SMB market segment.

Default policy modifications and policy updates are reported as somewhat awkward and can be confusing for the typical part-time administrators in an SMB environment.

The masking of sensitive data from unauthorized users in the management interface is still not supported.

The market in the low-complexity DLP deployments is becoming crowded with offerings from channel-DLP and DLP-lite solution providers (see The Trend for Channel-DLP and DLP-Lite section). Although Palisade continues to represent value to its client base, Gartner believes significant capability and pricing pressures for the new offerings will have a direct impact on Palisade's ability to grow its client base.

Return to Top

RSA, The Security Division of EMC

The offering from RSA, The Security Division of EMC, has had significant improvements since the previous content-aware DLP Magic Quadrant. Integration of the DLP solution with Archer and

NetWitness provides a notable value to clients already using these offerings within their environments. The updated UI appears to be the result of a deep review and analysis of how customers typically use the product. Although report capabilities have advanced, they are not quite yet at the stage where true risk-based reporting is available out of the box. The OEM agreement with Cisco's IronPort email encryption offering continues to be strong, and a simplified upgrade path from the IronPort RSA offering to the full RSA enterprise solution has been available since early 2012.

Strengths

- The stated RSA vision and product development plans are among the most complete of any vendor. If well-executed, they could present a serious challenge to Symantec over the next few years.
- Flexibility and scalability of RSA's data discovery capabilities continue to be among the best in the market.
- RSA has a strong focus on virtual desktop infrastructure and mobile with good virtualized environment capabilities. It demonstrated a clear understanding of the issues around DLP capabilities in the cloud.
- Its new management interface is significantly improved and provides new capabilities that are focused on assisting large organizational deployments, in addition to more comprehensive options for defining administrative roles.
- Reporting capabilities out of the box target line of business (LOB) audiences, in addition to other traditional audiences (for example, technology practitioners).

Cautions

- RSA is one of a few DLP solutions that do not digitally sign their logs and records, which is odd for a vendor with a strong focus on Archer and NetWitness integration.
- Substitution of sensitive information occurs during the presentation of the event record and is a weaker approach than some other vendors.
- The endpoint agent continues to be basic, and clients reported performance and accuracy issues with using some of the advanced content fingerprinting capabilities on the endpoint.

Return to Top

Symantec

Symantec retains a leadership position again for this year; however, the competition is closing the technical gap. The product offering continues to be composed of a solid base of components, and it also provides a strong mix of new features focused on integrating DLP capabilities in disruptive technologies, such as cloud, mobility and virtualized environments. Although Symantec had a significant focus on regulatory compliance deployment use cases in the past, product enhancements have pushed IP protection with this content-aware DLP offering as a strong value.

Its product road map vision has been developed with significant customer engagement and is among the most aggressive in this market. As a result, client expectations are very high for forthcoming enhancements. Although Symantec is similar to other vendors in that planned product road map features occasionally are delayed, the impact of these delays tend to be more compounded in the minds of Symantec clients. Clients are reminded to always consider any product acquisition based on existing functionality to ensure that all their requirements are met with the current capability set. Symantec's new CEO has indicated that the company plans to roll out new strategies in the first quarter. At this time, Gartner does not believe that these will impact Symantec's current content-aware DLP offering.

Strengths

- Content-aware DLP for tablets has been significantly improved and is one of the top capabilities discussed by clients.
- Content extraction capabilities have also been advanced and provide a more comprehensive solution to address IP protection deployments.
- Integration of native DLP capabilities within other Symantec products (such as Data Insight) is reported as a key acquisition criterion by clients.

Cautions

- Symantec has an impressive road map, but clients report concerns with on-time delivery of some road map features. Symantec explains that it prioritizes agility to new market conditions over a fixed road map; however, client expectations are not always recalibrated accordingly as changes occur.
- Although the management console is fully functional, it is no longer competitively the standout in Gartner-observed selections.
- Many of Symantec's reference customers complained to Gartner that support for the past 12 to 18 months has not fully met their expectations. Concerns were raised over trouble tickets remaining with first-line support for longer periods than would be expected before being escalated. Although Symantec has increased its support staff by 29% in 2012 over 2011 levels, it will take some time for the ramp-up to result in better satisfaction scores.
- Final deal pricing continues to be at the upper-premium end when compared to alternatives.

Return to Top

Trustwave

Trustwave obtained a comprehensive set of endpoint, network and discovery capabilities when it acquired Vericept in 2009; however, the product has seen very little in terms of updates or enhancements since. Trustwave targets the core compliance deployment market with this offering, which has remained very stable in terms of requirements in the past several years.

Strengths

- Core technology at the heart of the offering that can support complex use cases.
- Trustwave integrates its secure Web gateway, SIEM and content-aware DLP offerings into a single security solution.
- Its management console provides good dashboards and workflow.
- Although the offering comes with predefined regulatory compliance and acceptable use-case policies, the CANDL scripting language can be used to create custom policy sets; however, Trustwave's current target market will typically only leverage this capability in a minimal way.

Cautions

- Trustwave's product still does not support double-byte character sets.
- Gartner sees the Trustwave client base as focused primarily within regulatory compliance use cases and more specifically with a sweet spot on PCI requirements. Investment in product enhancements that would extend core capabilities beyond this target market has been minimal — thus, limiting its appeal to other potential clients.
- Its prepackaged suite of policies is limited. Additional policies are only offered on a demand basis.

Return to Top

Verdasys

Verdasys continues to focus on IP use cases with an offering that provides strong auditing and workflow. Management console integration with Fidelis appliances provides a fully rounded set of endpoint, network and discovery capabilities. A new managed service offering increases the appeal of the solution to organizations that do not want to operate a DLP solution in-house.

Verdasys has an OEM partnership with Fidelis, where Verdasys offers integrated Fidelis DLP and cyberthreat defense capabilities within its management console. Fidelis was acquired by General Dynamics in August 2012. General Dynamics, Fidelis and Verdasys have all stated publicly and to Gartner their joint intent to continue this relationship. Although there are always risks associated with acquisitions of this nature, it is Gartner's belief that the existing relationship will continue as is for at least the next 12 months.

Strengths

- Verdasys has a strong capability set for supporting complex IP protection deployments.
- Its new investigation module provides native capabilities for streamlining and supporting investigations.
- It offers advanced logging and auditing functions, and has built-in support for EU privacy controls.
- Its support for Linux and Apple desktops is a unique capability in this market.
- Verdasys offers strong support for virtualized environment deployments.
- Management console support to manage Fidelis appliances creates a full-featured offering with best-of-breed components.
- Verdasys has a managed service offering option for organizations that do not want to operate a DLP deployment.

Cautions

- Gartner clients have reported situations where some issues have taken a long time to resolve and that external assistance can be required to bring outstanding issues to resolution.
- Because of deep integration of Verdasys capabilities within endpoint OS and application environments, Gartner clients report that software updates and upgrades typically require more testing than with other software offerings to verify capability support and to ensure minimal impacts of changes on operations.
- Although General Dynamics has announced that the relationship between Fidelis and Verdasys — along with the current DLP road map — will not change, existing customers should understand that there are always the usual inherent risks during any change of ownership.

Return to Top

Websense

Websense's DLP offering has improved consistently for the past several years and has been among the most full-featured DLP solutions available in this market. It offers a good blend of endpoint, network and data discovery capabilities. This year, it has introduced enhanced capabilities to support mobile devices and also the ability to use advanced persistent threat features within the DLP solution to better evaluate risks.

Strengths

- Websense offers a full-featured DLP solution that supports endpoint, network and data discovery.
- Its "drip DLP" feature monitors for slow leaks of information over a long period of time.
- Websense has a strong policy engine with good remediation options.
- Its optical character recognition (OCR) capabilities identify sensitive content within scanned documents.

Cautions

- Its redaction capabilities are only supported for data at rest.
- Websense has been in a leadership role within the content-aware DLP market for several years; however, it appears to Gartner that its product road map is showing signs of slower feature adoption when compared to those of its competitors. This could impact its future appeal to clients and its overall position in the market.

Return to Top

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.

Return to Top

Added

- InfoWatch, based in Russia, is a new entrant in the 2013 Magic Quadrant.

Return to Top

Dropped

- Trend Micro has been in the process of winding down its stand-alone enterprise DLP solution and has announced end-of-sale for this product. Trend Micro has migrated to a strategy of embedding its DLP capabilities within its endpoint and gateway solutions. This is considered a channel-DLP approach and, at this time, does not meet the inclusion criteria for this Magic Quadrant.
- Safend was acquired by Wave Systems and did not meet this year's inclusion criteria.

Return to Top

Inclusion and Exclusion Criteria

This Magic Quadrant is restricted to enterprise content-aware DLP products.

Vendors are included in this Magic Quadrant if their offerings:

- Can detect sensitive content in at least two of network traffic, data at rest or endpoint operations
- Have a relatively sophisticated, centralized policy and event management console
- Can detect sensitive content using at least three of the following 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 29 February 2012

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

- Although Fidelis does not strictly meet these criteria because it is a network-only content-aware DLP appliance solution, we have included Fidelis in the Magic Quadrant for the following reasons:
  - Fidelis' product has a particularly impressive detection capability.
  - Client inquiries and deployments support Fidelis as being a viable alternative to enterprise DLP offerings.
  - The relationship between Verdasys and Fidelis is such that inclusion is warranted.

Vendors are excluded from this Magic Quadrant if their offerings:

- Use only simple data detection mechanisms (for example, supporting only keyword matching, lexicons or simple regular expressions)
- Have network-based functions that support fewer than four protocols (for example, email, instant messaging and HTTP)
- Primarily support DLP policy enforcement via content tags assigned to objects

Return to Top

Evaluation Criteria

Ability to Execute

Ability to Execute is ranked according to a vendor's ability to provide to the market a content-aware DLP product that meets customer feature/function capability requirements, as well as their ability to deliver and execute the product with a high level of service guarantee and customer support.

Vendor ratings are most influenced by the vendor's understanding of the market, its processes for soliciting customer feedback, and the experience of the customer. We also take into account the availability of solutions for emerging platforms, such as cloud and mobile devices.

Weights are subjective and contextual. Readers who conduct their own RFIs may choose to change weights to suit the needs of their business and their industry:

- **Product/Service** compares the completeness and appropriateness of core content-aware DLP technology capability. This is the most exhaustive of all of the assessed criteria.
- **Sales Execution/Pricing** compares the strength of a vendor's sales, partnerships, sales channels, deployment plans, pricing models and industry support.
- **Market Responsiveness and Track Record** reflects how vendors respond to customer feedback by assessing performance against previous product road maps, content of future product road maps and the cultivation of strategic advantages.
- **Customer Experience** is a combined rating of the materials provided to customers when they purchase the technology and, more significantly, what customers tell us about their experiences — good or bad — with each vendor.
- **Operations** assesses the ability of the vendor to provide support across all aspects of the customer engagement domain.

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 (January 2013)

Completeness of Vision

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.

Completeness of Vision is ranked according to a vendor's ability to show a commitment to content-aware DLP technology developments in anticipation of user wants and needs that turn out to be on target with the market. 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 that 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.

Our Completeness of Vision weightings are most influenced by four basic categories of capability: network performance, endpoint performance, discovery performance and management consoles. Weights are subjective and contextual. Readers who conduct their own RFIs may choose to change the weights to suit the needs of their business and their industry:

- **Market Understanding** is ranked through observation of the degree to which a vendor's products, road maps and missions anticipate leading-edge thinking about buyers' wants and needs. Included in this criterion category is how buyers' wants and needs are assessed and then brought to market in a production-ready offering.
- **Marketing Strategy** assesses whether a vendor understands its differentiation from its

competitors and how well this fits in with how it thinks the market will evolve.

Sales Strategy examines the vendor's strategy for selling products, including their pricing structure and their partnerships within the DLP marketplace.

Offering (Product) Strategy assesses the differentiation of its products from its competitors, and how it plans to develop these products in the future.

Innovation looks at the innovative features that vendors have developed to assess whether they are thought leaders or simply following the pack, and also the extent to which their products are able to combine with other relevant disruptive technologies.

Geographic Strategy is an assessment of the vendor's understanding of the needs and nuances of each region, and how the product is positioned to support those nuances.

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	High
Geographic Strategy	Standard

Source: Gartner (January 2013)

Quadrant Descriptions

Leaders

Leaders have products that work well for Gartner clients in midsize and large deployments. They have demonstrated a good understanding of client needs and generally offer comprehensive capabilities in all three functional areas — network, discovery and endpoint. They have strong management interfaces, and have tight integration with other products within their brand or through well-established partnerships and tight integration. They offer aggressive road maps and usually deliver on them. Their DLP products are well-known to clients and are frequently found on RFP shortlists.

Return to Top

Challengers

Challengers have competitive visibility and execution success in specific industry sectors that are better-developed than Niche Players. Challengers offer all the core features of content-aware DLP, but typically their vision, road maps or product delivery is narrower than the Leaders. Challengers may have difficulty communicating or delivering their vision in a competitive way outside their core industry sector.

Return to Top

Visionaries

Visionaries make investments in broad functionality and platform support, but their competitive clout, visibility and market share don't reach the level of Leaders. Visionaries make planning choices that will meet future buyer demands, and they assume some risk in the bargain, because ROI timing may not be certain. Companies that pursue visionary activities will not be fully credited if their actions are not generating noticeable competitive clout, and are not influencing other vendors.

Return to Top

Niche Players

A vendor is considered a Niche Player when its product is not widely visible in competition, and when it is judged to be relatively narrow or specialized in breadth of functions and platforms — or, for other reasons, the vendor's ability to communicate vision and features does not meet Gartner's prevailing view of competitive trends. Niche Players may, nevertheless, be stable, reliable and long-term vendors. Some Niche Players work from close, long-term relationships with their buyers, in which customer feedback sets the primary agenda for new features and enhancements. This approach can generate a high degree of customer satisfaction, but also results in a narrower focus in the market (which would be expected of a Visionary). In this Magic Quadrant, Niche Players may also be vendors that did not provide answers to all, or any, questions asked during the vendor survey.

Return to Top

Context

This Magic Quadrant is a market snapshot that ranks vendors according to competitive buying criteria. Vendors in any sector of the Magic Quadrant, as well as those not ranked on the Magic Quadrant, may be appropriate for your enterprise's needs and budget. Every company should consider content-aware DLP as part of its information security management program, so that the value of strategic information assets may be preserved and also so that the organization may avoid fraud, loss or harm arising from loss of other forms of sensitive information.

Return to Top

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 digital rights management protections. Content-aware DLP solutions provide capabilities to support regulatory compliance and IP use.

This is different from non-content-aware DLP solutions. These are often just referred to as "DLP" in vendor offerings. Non-content-aware DLP solutions apply a policy without reviewing the content or context of what is being monitored. As a result, these DLP solutions cannot adjust a policy response based on the content or context. An example of this type of capability is often found in USB port control tools. Technically, these tools can prevent the loss of data because they can block users from copying any and all information to a nonapproved USB drive, which is why they refer to this capability as a DLP solution. However, because these solutions cannot determine a difference in content or context, they do not offer any flexibility in the application of the policy. With a content-aware DLP solution that is used for USB control, a policy could be created so that a user would be able to save documents that do not contain any sensitive information on any USB drive, and save specific types of sensitive information (such as client data) only on a company-approved USB drive that has built-in encryption. Highly sensitive types of information (such as HR records) would not be allowed to be saved on any USB drive at all.

Content-Aware DLP Ought to Change Behavior

Used to its full capability, content-aware 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, which are unseen by end users. Nontransparent controls represent a cultural shift for many organizations, and it is critical to get business involvement in the requirements planning stages and as part of ongoing long-term operations of the content-aware DLP system. Specifically, the review of content-aware DLP events needs to be performed by LOB personnel versus IT or IT security personnel, because the LOB personnel are responsible for making a business decision on the acceptability of an incident within the business context.

As content-aware DLP tools mature, use cases for managing sensitive data are becoming more sophisticated. The use cases associated with virtualization, cloud, mobile and social media have become more common, as have 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 using a tablet or laptop while in a coffee shop or airport terminal. Features that support these use cases include endpoint and network content-aware DLP functions, as well as Web proxy integration and the ability to resolve a system to IP address or MAC address with a username. Support for these features have become common, but they do require integration with Microsoft Active Directory or other services.

Many vendors have begun experimenting with alternative delivery models such as cloud, software as a service and more traditional managed service offerings, where the vendor is responsible for setting up the system and ensuring that the policies meet client expectations. Gartner has had conversations with clients leveraging managed service offerings, and they report a typically faster time to value in their deployments versus traditional internally managed deployments. They also report that they are more willing to extend the initial scope of deployment and leverage more advanced use cases, because the vendor experience and support capabilities give them more confidence that the deployment will operate as they intended.

Fidelis Security Systems was acquired by General Dynamics in August 2012. This is the only major acquisition reported in the content-aware DLP market in more than two years. The last major acquisition was McAfee's acquisition of Reconnex.

Mobile Devices Still Pose a Challenge

Mobile devices — specifically tablets — have become commonplace within organizations; however, Gartner clients continue to report that they are struggling to establish appropriate terms of use and security overlays to manage and protect the sensitive information being accessed and used on these devices. Because of limitations in OS APIs, the variability of OS configurations, differing computing capabilities and battery life expectations, content-aware DLP vendors have not been capable of installing native content-aware DLP software natively on tablets or smartphones. Instead, they leverage mobile device management configurations to force a VPN connection back to the home network, where all traffic bound for sites external to the organization are scanned by the content-aware DLP network solutions they host at the perimeter of the network. This does not address the risks associated with a user disabling the VPN connection or tethering the mobile device to a third-party system, such as a home PC or via Bluetooth to removable media.

Virtualization, OS Support and Risk Reporting Are Still Lagging

The use of content-aware DLP for virtual environments has become more pronounced in the past 12 months; however, capabilities vary significantly among vendor offerings. Some do not support the installation of their DLP solution within a virtual machine, whereas others only support the scanning of virtual drives when not in use. Many of the current solutions involve the installation of vendor DLP solutions on each VM, as would be the case of a traditional physical system, rather than providing a common service layer. Cloud deployment of content-aware DLP solution also should be considered at an early stage of the deployment. Gartner expects this to change over the next 12 months, because most vendors reported aggressive plans for more advanced support of virtual environments in their product road maps.

Windows continues to be the OS of choice for vendor support in this Magic Quadrant. As in previous years, many vendors promised support for Apple's OS X if demand was high enough. Most vendors suggest they support OS X by being able to perform local data discovery using a network appliance or a software agent not locally installed on the OS X system. Only one delivered content-aware DLP capabilities that are deployed locally on the OS X system. Gartner does not anticipate that this situation will likely change for the next 12 to 18 months. Linux continues to be completely ignored by all but one vendor, and no other vendor has any plans for this platform. Until clients make it a buying criterion to have support for these platforms, vendors will continue to speak of them in future terms.

Content-aware DLP deployments are seen more and more as business tools by the businesses units themselves to address compliance and IP protection mandates than in the past, where it was often seen as an IT/IT security solution looking for a need. As a result, content-aware DLP business cases now typically include risk management as one of the cornerstone drivers; however, few vendor offerings support native reporting capabilities that are business- and risk-management-focused. Out-of-the-box reporting continues to be focused on listing the number and type of events that have been detected, rather than taking a risk-oriented view that looks at an 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 mindset that goes beyond linking reports to the way in which the content-aware DLP tool works to developing reports linked to the way in which they will be used outside of the IT and IT security departments.

Gartner Inquiry Data and Observations About Content-Aware DLP

Gartner inquiry data through 2012 indicates several major observations that should help organizations develop appropriate requirements and select the right technology for their needs:

- Gartner inquiries suggest that we are now getting beyond basic DLP use cases. DLP as a control for the protection of IP has been growing significantly, representing roughly 12% of all DLP inquiries up from 5% in previous years.
- The EMEA market, which has been difficult to navigate by content-aware DLP vendors — primarily because of regulatory compliance, privacy legislation and work counsel requirements — has begun to pick up, with notable advances in deployments in France, Germany, Switzerland, Russia, Turkey and Saudi Arabia.
- The trend for the Asia/Pacific region and Japan has primarily been for content-aware DLP deployments supporting IP protection; however, clients in some jurisdictions (such as Australia, India and Singapore) are primarily focused on regulatory compliance mandates.
- About 35% of enterprises led their content-aware DLP deployments with network requirements, 20% began with discovery requirements, and 45% started with endpoint requirements. Enterprises that began with network or endpoint capabilities nearly always deployed 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 their investments until they are capable of evaluating vendors' offerings against independently developed, enterprise-specific requirements.
- Furthermore, many organizations continue to make the mistake of assigning the daily management of content-aware DLP events to IT and IT security personnel, or they initiate their DLP solution deployment as part of an IT and IT security mandate, rather than focusing on establishing their DLP deployment as a business process.
- Although the primary appeal of endpoint DLP continues to be the protection of IP and other valuable enterprise data from insider theft and accidental leakage, there has been growing appeal in the past 12 months for the use of endpoint DLP to address regulatory compliance use cases.
- Most content-aware DLP solutions continue to focus on text-based content in their analysis. Although there were significant capability updates by a few vendors for OCR support, chemical formula notation support and schematic analysis, most vendors still struggle with nontext data — even with fingerprinting support.
- Lack of support for fingerprinting on endpoints continues to be the dirty little secret of the industry. Although a few vendors offer this capability in some form, the majority that do only support a coarse initial high-level scan at the endpoint and then leverage a phone home

capability to a locally available network appliance for the actual fingerprint matching analysis.

Many deployments are sold on the basis of being a tool to assist in risk management activities; however, most content-aware DLP solutions do not offer reporting, dashboard or even generalized feedback relevant for this function.

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

The Trend for Channel-DLP and DLP-Lite Solutions

There is a growing market trend for DLP-enabled offerings to support many components making up an enterprises' IT ecosystem. Some vendors provide content-aware DLP capabilities that are quite advanced, while others only support basic registered expression matching. The following list of vendors represents an overview of the types of channel-DLP and DLP-lite solutions that Gartner will investigate in future research:

- ContentKeeper Technologies
- Identity Finder
- NextLabs
- Proofpoint
- Raytheon Oakley Systems
- Sophos
- Wave Systems
- Workshare
- Xbridge Systems
- Zscaler

Additional research contribution and review were provided by Rob McMillan.

Return to Top

About Gartner | Careers | Newsroom | Policies | Site Index | IT Glossary | Contact Gartner