Gartner

Magic Quadrant for Content-Aware Data Loss Prevention

12 December 2013 ID:G00253215

Analyst(s): Eric Ouellet

VIEW SUMMARY

Enterprise content-aware DLP has evolved to integrate more contextual awareness, enabling broader deployment use cases beyond regulatory compliance and intellectual property protection. Typical clients are organizations operating in regulated industries, intellectual property firms and governments.

Market Definition/Description

Gartner defines content-aware DLP technologies as those that 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 for this Magic Quadrant, products must support sophisticated detection techniques that extend beyond simple keyword matching and regular expressions, and must be considered enterprise DLP solutions, as described below.

Content-aware DLP technologies can generally be 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; as physical and virtual appliances for monitoring networks; and as agent software, soft appliances, virtual appliances and physical appliances for data discovery. Some of the leading differentiating characteristics of enterprise content-aware DLP solutions include a centralized management console for all the provided components, support for advanced policy definition and event management that supports complex workflows.
>
> **DLP-lite** products typically use fewer and less-sophisticated detection techniques, and support only a limited number of protocols (for example, email, Web and FTP). Deployments tend to be exclusively at the endpoint or at the network perimeter, or in support of 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). In this mode, channel DLP 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, the system can automatically determine 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.

During the past years, the enterprise content-aware DLP market has continued to experience steady growth, with content-aware DLP market revenue growing from $369 million in 2010 to $458 million in 2011 to $572 million in 2012. Gartner's current estimate is that this market will reach between $680 million and $710 million in 2013, and is estimated to grow an additional 22% to 25% by the end of 2014, to reach approximately $830 million.

Return to Top

Magic Quadrant

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

STRATEGIC PLANNING ASSUMPTION

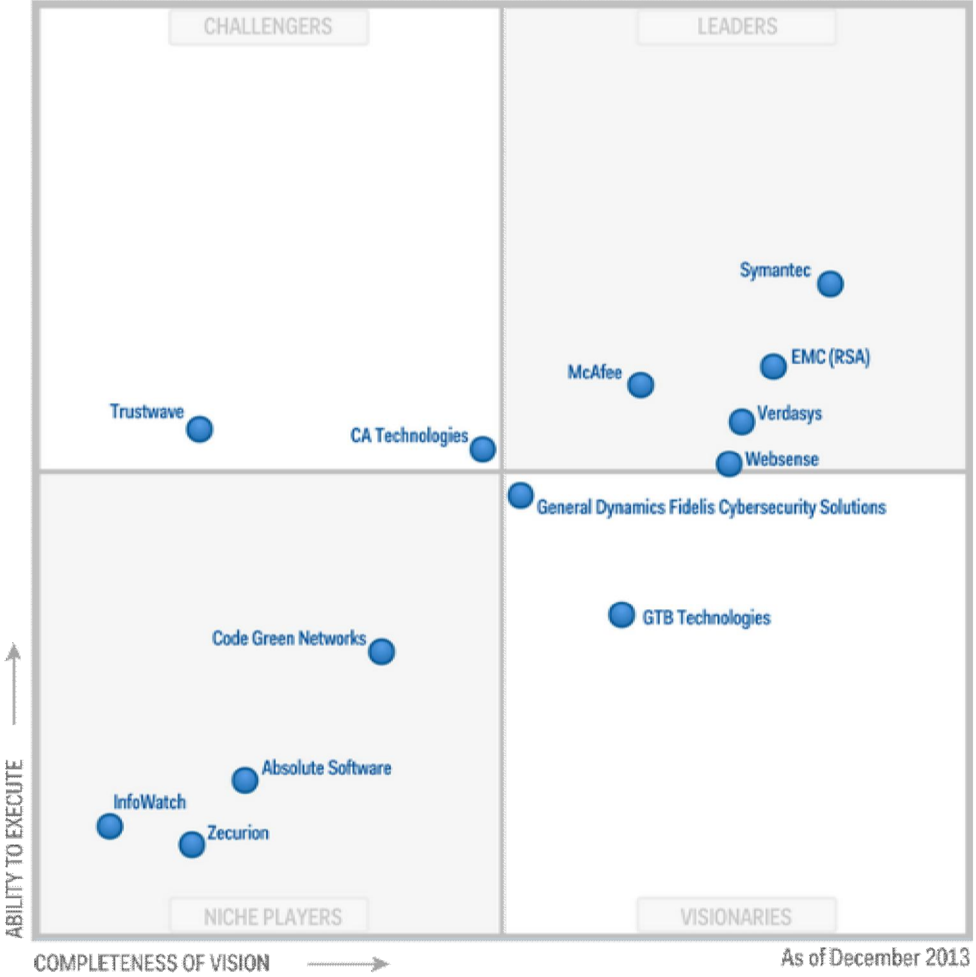
By 2015, as the focus of data loss prevention (DLP) deployment efforts shifts from compliance to broader business protection, context awareness will become the leading feature of DLP solutions.

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 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



Source: Gartner (December 2013)

Return to Top

Vendor Strengths and Cautions

Absolute Software

Absolute Software acquired Palisade Systems in July 2013, and the product is now called Absolute DLP. At the time of this research, the acquisition was too recent to have a material impact on the product offering; this assessment is provided on that basis.

While the product capabilities remain firmly within the baseline of the traditional small or midsize business (SMB)-focused regulatory compliance segment of content-aware DLP deployments, the product has fallen behind other SMB-focused competitive offerings, due to extremely limited investment in capability enhancements in prior years.

The offering supports network, endpoint and agent-based discovery functions. The 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 a presence in the healthcare, financial services and education sectors.

Strengths

The acquisition by Absolute Software signifies a positive direction for the product. With planned integration of existing Absolute Software capabilities during the next 18 months, and direct access to a significantly larger customer base, Absolute Software has opportunities to significantly mature the offering, which will be a net benefit to existing and future clients.

Simplicity of deployment and integration with Web and email security services remains a high note for Absolute DLP clients.

Cautions

Although the product is baseline-feature-competitive within the SMB space, the overall offering has suffered from a significant lack of investment in the development of new capabilities during the past several years. While the acquisition by Absolute Software represents an opportunity, there is a risk that planned road map deliverables can be delayed due to technical and other factors.

Clients have reported less success than in previous years regarding resolution of technical issues with the vendor; combined with a lack of product evolution, this has been a considerable factor in clients switching to alternative solutions.

Gartner assesses that the management interface does not provide a simple or comprehensive view of an organization's deployment. The interface requires considerable click-throughs to access common functions, reports are generated on demand, and the interface is not as intuitive or as easy to use as it should be for an offering targeting the SMB market segment.

The market in low-complexity DLP deployments is growing, with many new offerings from channel DLP and DLP-lite solution providers (see The Growing Market for Channel DLP and DLP-Lite Solutions section). Gartner believes significant capabilities and pricing pressures for the new offerings will have a direct impact on this product's appeal to new clients.

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

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

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

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

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

Completeness of Vision

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

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the 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 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.

Return to Top

CA Technologies

CA Technologies continues to have a well-rounded offering, and in the past 12 months, it has improved core and advanced capability sets with a good balance of content and context awareness. The key buying criterion quoted most by CA DataMinder clients observed by Gartner continues to be an existing relationship with CA.

Integration with other CA products, such as SiteMinder and IdentityMinder, has a strong appeal with existing CA clients. This integration will feed the growth in adoption of CA products within existing CA accounts.

Strengths

- CA DataMinder provides comprehensive policy packs with globally localized variants.
- The link between identity management and DLP continues to be a highlight of the solution.
- Event logs are stored in a tamper-proof encrypted and compressed database with protected access control.
- Support for messaging infrastructures remains a strong value point for highly regulated industries.

Cautions

- While endpoint agents support unstructured data fingerprinting, they do not support structured data fingerprinting as a means of discovering content.
- CA continues to lack OS X support, and it is not on the road map for the upcoming release. The vendor is considering support within a future release; however, this would leave it several years behind even significantly smaller competitors, which now offer basic and advanced functionality for OS X.
- CA DataMinder product clients report again this year that policy and event management functions continue to be complex, and require specialized training and experience to achieve a level of comfort and competence for both technical and nontechnical business users.
- CA DataMinder does not offer discovery of sensitive data stored in the cloud within email providers (Office 365, Gmail), SharePoint Online or cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.).
- Gartner believes that CA continues to have limited appeal to organizations that are not current clients. The value of the DLP offering is maximized when leveraging other integrated CA products.
- Clients report that obtaining technical support can be cumbersome. The process required to log trouble tickets is more involved than it should be, and the wait time to obtain a resolution is long.

Return to Top

Code Green Networks

Code Green Networks continues to lag behind in market penetration and growth, compared with market trends and other vendors in this space. Furthermore, client inquiry and market trends are showing that, over time, Code Green Networks is becoming more associated as a competitor among DLP-lite and integrated DLP solution providers, versus a direct competitor in the enterprise DLP market. This distinction is one that the vendor must shed if it is to continue to be relevant in the enterprise content-aware DLP market.

While the product set is relatively comprehensive for a vendor of its size, and Code Green Networks has a clear focus on a simple-to-use approach, clients are reporting growing concerns regarding support of more advanced use cases.

Strengths

- The vendor offers attractive pricing for its market segment and the capabilities provided.
- Social media support is provided for Facebook, Twitter and Myspace, as well as for hybrid cloud integration, including a relationship with Box.net.
- There is support for Citrix XenApp and XenDesktop for Windows clients, along with XenServer server-side deployments.
- Good overall enhancements make the current product version easier to use than previous solutions.
- Clients report that solution cost, ease of use, available features and time to implement are key buying considerations for Code Green Networks.

Cautions

- While the vendor offers an OS X and a Linux client, both are currently limited to data discovery functions only.
- A lack of advanced features (such as supporting contextual awareness from alternate sources) limits deployments to typical baseline DLP use cases.
- Code Green Networks attempts to communicate its value proposition to larger enterprises; however, its lack of investment in risk compliance and advanced contextual awareness is limiting its appeal beyond the mainstream, low-complexity regulatory compliance market segment.
- Clients report concerns regarding support due to the very limited number of senior-level technical resources from the vendor, and the time it takes to troubleshoot complex issues as a result.
- Clients have expressed concerns over the longer-term availability of knowledgeable staff in critical areas, and the impact this could have on development, operations and support.

Return to Top

EMC (RSA)

The offering from RSA, The Security Division of EMC, continues on its product innovation path, and with integration with other EMC components. The focus of the solution is on incorporating contextual information (such as threat intelligence, behavioral analytics and risk insight) within the framework of DLP to better support regulatory compliance and intellectual property (IP) protection mandates. Many clients report that one of the great appeals of RSA as a DLP provider is its independence from typical endpoint protection offerings, making it an interesting proposition for clients that do not wish to further their relationship with an existing vendor.

The OEM agreement with Cisco's IronPort email encryption offering is mature at this stage. While IronPort clients report overall satisfaction with the capabilities provided via this relationship, the upgrade path to RSA's full enterprise DLP offering is still not a major revenue source for RSA. Gartner believes this relationship is still very valuable to both organizations' clients and will remain an available offering in the longer term.

Strengths

- A managed security service for the RSA DLP option is available.
- Strong context-aware governance, risk and compliance (GRC; Archer and NetWitness) and security analytics integration with DLP provide notable value to clients already leveraging these solutions internally.
- The RSA embedded DLP solution in Cisco IronPort can be managed from the RSA console.
- Policies supporting data fingerprinting on the endpoint do not require tethering. They continue to operate when the agent is disconnected from the home network.
- The flexibility and scalability of RSA's data discovery capabilities — which include the creation of a grid of resources with automated load balancing and distribution of content for analysis to its members, along with full and incremental sampling — continue to be among the best in the market.
- There is Citrix XenDesktop and XenApp, VMware View and Microsoft Hyper-V virtual desktop support, including local removable media support.
- The stated RSA vision and product development plans continue to be among the most comprehensive of any vendor.

Cautions

- Endpoint DLP does not support print screen functionality.
- Although RSA provides SharePoint Online discovery support, it still lacks support for the discovery of sensitive data in the cloud within hosted email providers (Office 365, Gmail) or within cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.).
- RSA continues to be one of the few vendors that does not digitally sign log records. While the vendor claims that clients do not ask for this feature specifically, the lack of it is extremely puzzling, considering RSA's significant presence as a provider of cryptographic functions to many third parties, and its strong product emphasis on governance and compliance.
- The endpoint agent continues to be basic, and clients report performance and accuracy issues with some of the advanced content fingerprinting capabilities on the endpoint.
- RSA continues to claim that OS X support is on the road map, as it has claimed for several years; however, such support has yet to materialize as an available option. Even significantly smaller competitors now offer basic and advanced functionality for OS X.

Return to Top

General Dynamics Fidelis Cybersecurity Solutions

The Fidelis XPS solution continues its evolution, providing the market with the leading network-focused DLP solution. A strong emphasis on integrating DLP with solutions that address insider threats, zero-day exploits, advanced persistent threats and other data breach vectors continues to make the solution appealing to organizations in need of a high-end DLP solution.

Fidelis has an OEM partnership with Verdasys, where Verdasys has the ability to manage the Fidelis XPS DLP solution and cyberthreat defense capabilities within its management console. A year after the General Dynamics acquisition of Fidelis Security Systems, the Verdasys relationship and collaboration appear to continue to be strong. At this time, the Fidelis offering remains a core component of the Verdasys-managed DLP service offering.

Strengths

- The Fidelis XPS product has one of the strongest content inspection and network throughput capabilities available in a content-aware network DLP offering.
- Its differentiating approach emphasizes protection from external threat sources by integrating contextual awareness with traditional content-aware DLP.
- Fidelis XPS's ability to actively prevent data leaks natively, without requiring a third-party proxy, is a differentiator that appeals to its customer base.
- Clients report that the vendor is very responsive to support requests and feature updates, and that they are very satisfied overall with their investment in the product.
- Clients report a predictable cadence of releases as a key valued benefit of working with the vendor.
- The Fidelis XPS solution is available as a managed service via the Verdasys managed service offering.

Cautions

- The Fidelis XPS offering continues to be available at a premium, when compared with other offerings.

The product is limited to network DLP only. Organizations requiring endpoint agents to control local actions or data discovery capabilities must use Verdasys — the preferred partner — or an alternate agent DLP solution.

A continued focus on and investment in threat detection (such as advanced persistent threats, among others) could take the focus away from the vendor's core DLP offering.

Although the management console continues to improve, and provides all the necessary information, it remains a weak point in the overall offering, requiring significant clicking and scrolling to view or access all the information.

Return to Top

GTB Technologies

GTB Technologies provides a comprehensive content-aware DLP solution with endpoint, network and data discovery solutions that incorporates additional contextually aware capabilities, resulting in a well-rounded solution with distinct appeal to SMBs with advanced protection requirements, such as the control of IP. GTB is one of the few vendors that support a managed service offering deployment option.

Strengths

Use of advanced data fingerprinting as the leading detection mechanism can provide higher fidelity with intellectual-property-focused use cases.

There are flexible deployment options available, including multitenant, managed service, virtualized and cloud (such as Azure and Amazon Web Services [AWS], among others).

There is support for discovering content within cloud storage environments, such as Box.net, Dropbox, SkyDrive, Google Drive, Huddle and CloudAccess.net, among others.

GTB is among a very small set of content-aware DLP vendors that have integrated enterprise digital rights management/information rights management remediation capabilities directly within their DLP solutions.

Clients report a very positive overall experience with GTB's customer support organization, and that the vendor is very responsive to capability and feature enhancement requests.

The cost-benefit, with favorable pricing for the available capability set, is the most quoted buying criterion by clients.

Cautions

GTB continues to lack network monitoring capabilities on the endpoint.

When offline, the endpoint client only supports pattern detection using extended regular expression matching. Integrated offline fingerprinting and network monitoring are on the product road map for 2014.

Network-based data discovery is limited to a Microsoft Software Installer package, which can be installed on Windows systems. GTB does not currently offer the discovery functionality as a vendor-supplied hardware appliance, soft appliance or virtual appliance.

Native cloud support is still lacking. While GTB offers data-in-motion scanning, it does not offer discovery of sensitive data in the cloud within hosted email providers (Office 365, Gmail), SharePoint Online or cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.).

Return to Top

InfoWatch

In its second year in the content-aware DLP Magic Quadrant, the InfoWatch content-aware DLP offering is still in an early stage of development, when compared with the leading vendors in this market. The vendor currently has a geographic focus and partner ecosystem firmly based in Russia, EMEA and some parts of Asia. Customer references continue to be happy overall, but highlight the need for the product to evolve to ensure continued value and relevance in client deployments.

Strengths

Forensic capabilities are supported by shadow copy files forwarded to the central server when an action with sensitive data triggers a DLP rule on the endpoint.

The product supports the fingerprinting of sensitive data, and includes dedicated capabilities for scanning and detecting official documents and stamps (such as passport entry stamps).

There is support for Microsoft Office and OpenOffice formats, along with graphic objects, audio and video files, and computer-aided design (CAD) formats

Cautions

Although the vendor's 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 use either to create their own policies or to engage with the vendor to build policies on their behalf.

Network scanning is primarily focused on HTTP traffic only. Cloud use cases are not currently supported.

The agent does not have native content analysis capabilities and relies on the gateway to perform these operations.

The limited system integrator ecosystem limits client deployment scenarios to geographies that are existing strongholds, and reduces the appeal of the offering in other regions.

The management console and policy engine continue to be areas in need of improvement. While the interfaces are relatively clean and intuitive for technically savvy users, they are currently not designed for large deployments or scenarios where there would be significant event activity.

The offering lacks maturity in terms of documentation and deployment best practices.

Return to Top

McAfee

McAfee is owned by Intel. The key buying criteria quoted most by McAfee DLP clients continue to be: (1) an existing relationship with McAfee; (2) the integration with McAfee ePolicy Orchestrator (ePO); and (3) the event capture database. This capture database, a centralized inventory of activity data used in the testing and streamlining of new policies to address possible false positives and to reduce deployment time, remains a unique feature within the industry.

As in previous Magic Quadrants, overall customer satisfaction continues to be a point of concern for McAfee. While improvements have been made, and it is expected that large vendors in any industry will have customer churn for a number of reasons, Gartner continues to receive a steady flow of inquiries regarding alternatives to, or replacement options for, McAfee DLP. Reasons quoted range from issues with technical support resolving deployment problems to the slow pace of long-term feature and policy integration between the component products.

Strengths

Integration with McAfee Enterprise Security Manager (formerly Nitro Security) provides real-time analytics from McAfee product sources, including global threat landscape input to the DLP solution for added contextual insight at the decision point.

LDAP and Active Directory integration enable the building of complex context-related rules for the support of International Traffic in Arms Regulations (ITAR) and data-residency-sensitive deployments.

DLP integration within McAfee Web Gateway proxy supports decrypt and re-encrypt of Web traffic for DLP content inspection including Box.net, SkyDrive and Google Drive.

The offering supports automated e-discovery requests from Guidance (encase) and AccessData products directly to the McAfee management system.

Supports the active decryption and DLP review of content protected using McAfee's own encryption solution.

There is integration with Microsoft Rights Management Service (RMS), Seclore, TrueCrypt and Titus as active remediation options.

There is integration with McAfee ePO.

Cautions

While the endpoint and network events are unified in the console, the endpoint and network continue to be managed independently. The client manager is not as refined or intuitive as the network manager, and has a bulky feel when there is a lot of data to be displayed. This is a key area of integration that should have become consistent by now, considering that the component product acquisitions occurred well over four years ago.

Although in previous years support for attaching documents was available, the current product does not support attaching documents that were not part of the original event within the workflow.

Native cloud support is still lacking. McAfee does not offer discovery of sensitive data in the cloud within hosted email providers (Office 365, Gmail), SharePoint Online or cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.).

McAfee continues to claim that OS X support is on the road map, as it has claimed for several years, but it has yet to materialize as an available option. Even significantly smaller competitors now offer basic and advanced functionality for OS X.

Reliance on system root-user access for management is an ongoing concern.

The logging of access to the system and the automated backup solution, while functional and adequate for many deployments, could benefit from enhancements targeted to larger, geographically dispersed and complex deployment clients.

There is no managed service offering currently available.

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

Return to Top

Symantec

With an emphasis on expanding the appeal of its DLP solution to use cases beyond traditional regulatory compliance, Symantec features context-aware integrations that will benefit clients concerned with IP protection and business-oriented topics, such as the threats from well-meaning insiders and malicious insiders. The available comprehensive functionality, along with the product's significant adoption in the marketplace, positively impacts the overall rating for Symantec.

The direct competition, which now more regularly includes smaller niche players, continues to steadily close the technical gap. Symantec must both increase the rate of integration within its own broad ecosystem of solutions and seek increased integration with high-value third parties to create value multipliers for existing and potential clients.

Strengths

The increasing focus on the integration of context-aware capabilities within the Symantec DLP offering is pushing the deployment of DLP beyond regulatory compliance to broader business protection frameworks.

Symantec is the vendor with the largest share of regulatory-compliance-focused content-aware DLP deployments. This deployment experience has resulted in one of the most detailed and tested deployment methodologies (the DLP maturity model) currently in use in this market.

Symantec has the single largest dedicated DLP team in this market — specifically in terms of development, support and service staff. The Symantec DLP group also has the distinction of having the single largest head count increases in the past 12 months.

Symantec's staff augmentation services offer organizations the opportunity to hire a dedicated resident content-aware DLP expert from Symantec. Multiyear managed services and hybrid SaaS offerings can also be obtained from Symantec. These approaches can significantly reduce the time to value of a content-aware DLP deployment.

Cautions

Symantec currently does not support the discovery of content stored within multitenant cloud hosted email services (such as Gmail or Office 365), and relies on scripts to send copies of data uploaded to cloud storage environments (such as Box.net, Dropbox, SkyDrive and Google Drive) to the Symantec DLP solution for inspection.

Exact-match fingerprinting and content-registration-based rules are not evaluated locally on the endpoint agent; they continue to rely on a phone home capability to the Symantec Endpoint server for exact match analysis. The agent locally evaluates content against fingerprints based on vector machine learning.

Clients continue to be concerned with the overall deployment complexity of the core infrastructure components of the Symantec DLP solution, when compared with competing solutions.

Symantec continues to claim that OS X support for basic local data discovery is on the road map, as it has claimed for several years, but it has yet to materialize as an available option. Even significantly smaller competitors now offer basic and advanced functionality for OS X.

Return to Top

Trustwave

While Trustwave officially opted out of actively participating in this Magic Quadrant, Gartner client interest in this solution has maintained a steady state and the product continues to meet the inclusion criteria. Thus, it is included in this analysis. Gartner compiled data based on public and private sources to evaluate the current product release.

Although the solution continues to have a comprehensive core set of endpoint, network and discovery capabilities, the product suffers from an infusion of only minor updates and enhancements targeting Trustwave's core compliance deployment market.

Strengths

The core content-aware DLP technology at the heart of the offering is well-adapted to support complex deployment scenarios supporting advanced regulatory compliance and IP protection use cases.

Trustwave integrates its secure Web gateway, security information and event management (SIEM) and content-aware DLP offerings into a single security solution, which clients have reported as a key buying criterion for the solution.

Although the offering comes with predefined regulatory compliance and acceptable use case policies, the Content Analysis Description Language (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 continues to be minimal, thus limiting its appeal to other potential clients who would be interested in this solution.

The vendor's prepackaged suite of policies is limited. Additional policies are offered only on demand.

Return to Top

Verdasys

While the Verdasys Digital Guardian DLP solution can be found deployed in regulatory compliance use cases, the bulk of deployments continues to be focused on the protection of IP and trade secret use cases with an offering that provides strong auditing, workflow and sensitive content protection. The integration of consumable context-aware information from both internal and third-party sources as part of the product's decision-making framework is elevating deployment applicability to broader business protection use cases within the enterprise.

Verdasys has an OEM partnership with General Dynamics Fidelis Cybersecurity Solutions, whereby Verdasys has the ability to manage the Fidelis XPS DLP solution and cyberthreat defense capabilities within its management console. A year after the General Dynamics acquisition of Fidelis Security Systems, the Verdasys relationship and collaboration appear to continue to be strong. At this time, the Fidelis offering remains a core component of the Verdasys managed DLP service offering.

This analysis is based on the combined Verdasys and General Dynamics Fidelis Cybersecurity offering available from Verdasys.

Strengths

Both a customer-owned-and-operated solution and a range of managed service offerings are available from and operated by Verdasys. The General Dynamics Fidelis Cybersecurity offering is available as an add-on component for these solutions.

Integration of unified enterprise encryption with Digital Guardian provides policy-driven encryption on local endpoints, servers, removable media, and email and its attachments. Microsoft RMS is also supported.

Verdasys has a strong capability set for deployments supporting the protection of complex IP and trade secrets from insider threats, cyberthreats, and advanced persistent threats via a hardened and highly tamper resistant endpoint, as well as the forensic logging of all endpoint activities.

The offering's advanced capabilities supporting both Linux and OS X desktops are unique in this market.

Management console support to manage Fidelis appliances and Titus user classification solutions creates a full-featured offering with best-of-breed components.

Cautions

Structured data fingerprinting is not supported on the endpoint agent.

Structured data discovery is only supported for Microsoft Access and IBM Notes. No Open Database Connectivity (ODBC) connector is available at this time.

Discovery of cloud stored data is limited to Box.net and SkyDrive. Dropbox and Google Drive are currently not supported.

The agent software has deep integration with low-level OS functionality, which can result in performance and functionality impacts on other applications, especially when employing baseline endpoint hardware configurations.

Furthermore, Gartner clients continue to report that software updates and upgrades typically require more testing than other software offerings to verify capability support and to ensure minimal impacts of changes on operations.

Clients express concern with the overall complexity of the DLP deployment and report that day-to-day operations require a very steep learning curve to reach a level of competence with the product, when compared with competing offerings.

Return to Top

Websense

Websense's Data Security Suite DLP offering provides a good blend of endpoint, network and data discovery capabilities. The vendor has a good balance of client deployments, including typical regulatory compliance, business-sensitive information and advanced IP protection.

While Websense introduced new DLP capabilities in 2013 that have broad appeal to a diverse prospect base, the vendor's continued approach to sales and client deployment support via its traditional Web and email security gateway partner ecosystem again raises concerns with clients and even other resellers. Successful content-aware DLP deployments are business-process-centric, and require resellers or system integrators with the skill set, experience and seasoned understanding to navigate thorny business issues to ensure successful and meaningful deployments. Not all resellers or system integrators are created equal. Potential Websense DLP clients are advised to verify that their shortlist deployment partner has referenceable and successful Websense DLP deployments that match their intended regulatory compliance and/or IP deployment use cases.

Strengths

Websense leverages the Triton architecture to centrally manage its DLP offering alongside Websense's Web and Email Security Gateways, and to provide context-aware data feeds to the DLP decision process.

Websense is among the few vendors that offer OS X endpoint agent support, which includes data discovery, application control, removable storage, optical media, Web and email traffic.

Websense also offers a Linux agent that supports data discovery and the monitoring of file transfers to removable media.

Clients note the following as key buying criteria for selecting the vendor's solution: (1) an existing relationship with Websense; (2) favorable pricing for the capability set; and (3) low complexity of deployment.

Cautions

Native cloud support is still lacking. Websense does not currently offer the discovery of sensitive data natively in the cloud within hosted email providers (Office 365, Gmail), SharePoint Online or cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.). Cloud support is currently only supported via the agent for data that is in motion to the cloud.

Clients report issues with Websense client support ranging from long delay times to obtain resolutions to limited availability of senior technical product resources to meet requests.

Local deployment support is also a concern raised by clients and even other resellers. The leading issue involves the variability of local resellers' overall capabilities and their ability to successfully support business-focused content-aware DLP deployments. Potential clients must verify that their chosen partner has the proper skill set for their deployment needs, and that reference clients match their deployment goals and are, in fact, satisfied with the services rendered.

Return to Top

Zecurion

Zecurion, based in Russia, is a new entrant to this Magic Quadrant and aims to address regulatory compliance and IP protection use cases. The Zecurion solution provides three components: the Zlock endpoint, the Zgate network and the Zdiscovery agent for data discovery. Currently, the majority of existing clients are in Russia, former Soviet Union countries and Eastern Europe; however, Zecurion is expanding into the U.S. market and has established a local office and relationships with key resellers to market and support its solution.

Strengths

- The solution provides full archiving of all data extracted from the endpoint on USBs, CDs/DVDs, printers, email and Internet communications, and can also capture screen shots.
- An extensive set of baseline data dictionaries is used as the basis for developing rules.
- There is an optical character recognition capability for identifying content.
- The solution provides interfaces to monitor social media, Web and cloud storage interactions.
- Pricing and configurations are SMB- and large-enterprise-friendly.

Cautions

- The offering is still at an early stage of development, and will require more integration and development from the vendor to address complex use cases.
- The management interface is usable, but is currently not designed to support large deployments or nontechnical users. Specific events can be difficult to locate within the management interface, which can quickly run out of display room when drilling down on an event.
- Zdiscovery is a reconfigured endpoint discovery agent adapted for SMB/Common Internet File System (CIFS) server share scanning, which is limited in scalability and throughput when compared with competing vendor offerings.
- Endpoint does not currently support exact document matching, partial document matching, structured document fingerprinting or statistical analysis.
- Clients require significant product configuration to support advanced use cases.
- Native cloud support is lacking. Zecurion does not offer discovery of sensitive data in the cloud within hosted email providers (Office 365, Gmail), SharePoint Online or cloud storage environments (Box.net, Dropbox, Google Drive, SkyDrive, etc.).

Return to Top

Vendors Added and 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

- Absolute Software (the vendor acquired Palisade Systems)
- Zecurion

Return to Top

Dropped

- Palisade Systems (the vendor was acquired by Absolute Software)

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 operations: network traffic, data at rest or endpoint
- 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: 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 communications
- Were generally available as of 30 June 2013

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

- Although the Fidelis offering does not strictly meet these criteria (because it is a network-only content-aware DLP appliance solution), we have included General Dynamics Fidelis Cybersecurity Solutions in the Magic Quadrant for the following reasons:
  - Fidelis 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 General Dynamics Fidelis Solutions 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)

Their offerings have network-based functions that support fewer than four protocols (for example, email, IM and HTTP)

Their offerings primarily support DLP policy enforcement via content tags assigned to objects

Their DLP offerings are embedded within other suites or products and are not available in a stand-alone form

Return to Top

Evaluation Criteria

Ability to Execute

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

Weightings are subjective and contextual. Readers who conduct their own RFIs may choose to change weightings to suit the needs of their businesses and industries:

Product or Service compares the completeness and appropriateness of the 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/Record reflects how vendors respond to customer feedback by assessing performance against previous product road maps, the 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 or Service	High
Overall Viability	No Rating
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	No Rating
Customer Experience	High
Operations	High

Source: Gartner (December 2013)

Return to Top

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. We continue 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 the 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 crossing 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. Weightings are subjective and contextual. Readers who conduct their own RFIs may choose to change the weightings to suit the needs of their businesses and industries:

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 is how buyers' wants and needs are assessed and 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 its pricing structure and its partnerships in the DLP marketplace.

Offering (Product) Strategy assesses the differentiation of a vendor's 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	Medium
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Medium

Source: Gartner (December 2013)

Return to Top

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 brands 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 and/or product delivery is narrower than those of Leaders. Challengers may have difficulty communicating or delivering on their vision in a competitive way outside their core industry sectors.

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 particular Magic Quadrant, Niche Players may also be vendors that did not provide answers to all, or any, of the questions asked in 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

Noise about DLP capabilities is at an all-time high. As the market for DLP solutions continues to experience accelerated growth, many vendors of security-related solutions are offering (or simply claiming) DLP capabilities within their product portfolios. Buyers should be skeptical of DLP-related marketing until it has been verified or substantiated. Most DLP solutions do not have any content-awareness capabilities, and those that do, at best, have limited and extremely basic pattern matching — yielding significant false positives when attempting to match data. Nearly all these offerings have extremely limited integration, if any, to support automated remediation, and most do not have any form of event workflow.

The content-aware DLP tools covered in this research support the dynamic application of a policy, based on the analysis of content determined at the time of an operation. Content-aware DLP describes a set of technologies and inspection techniques that are 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. The content-aware DLP solutions mentioned in this research all have the basic capabilities to address typical deployment use cases.

This is different from non-content-aware DLP solutions or simple DLP solutions, often referred to as just "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 non-approved USB drive, which is why this capability is referred to 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. When a content-aware DLP solution is used for USB control, a policy could be created so that a user would be able to:

- Save documents that do not contain sensitive information on any USB drive.
- Save specific types of sensitive information (such as client data) only on a company-approved USB drive that has built-in encryption.
- Prevent the saving of highly sensitive types of information (such as HR, client and patient records) on any USB drive.

Return to Top

The Continuing Evolution of Content-Aware DLP

By 2015, as the focus of leading DLP deployment efforts shifts from typical compliance to broader business protection, context awareness will become the leading feature of DLP solutions.

This is in line with adoption trends and the use cases reviewed during the past 18 months. While a portion of the DLP market continues to want simple regulatory compliance checkbox solutions for credit card, health and other sensitive client data, most of the organizations in that market are not looking for a comprehensive offering. They are looking for an add-on capability in an already existing component within their environment to address their DLP needs within very few use cases — typically email and Web, and occasionally removable media — and thus should continue to consider channel DLP and DLP-lite offerings.

As DLP deployments evolve from reactive protection within the first couple of years of deployment to an advanced proactive-protection-based model, contextual information becomes a critical core component. Leading organizations considering the current crop of enterprise content-aware DLP solutions will go beyond the basic regulatory compliance use cases and will have plans for one or more the following scenarios, among many others:

- Enhanced data governance
- Policy-based data access control
- A range of remediation options, based on the context of use, risks and threats
- Intelligent business process integration
- Active IP protection
- Malicious insider threats
- Protection from data loss in software and storage as a service, along with the integration of other cloud offerings
- Zero-day attacks targeting sensitive data

Requirements for these scenarios can only be addressed properly within a DLP framework when the context of use before, during and after is clearly understood. This has resulted in enterprise content-aware DLP vendor offerings evolving to integrate diverse sources of contextual information, ranging from basic integration with identity sources — something that has been available for many years — to broader integration with security incident and event management, entitlement attribution solutions, threat detection networks, network access control solutions, configuration management, fraud detection capabilities, and other sources.

Return to Top

Context-Awareness as a Means of Improving the Accuracy of Automation of DLP Solutions

Content-aware DLP solutions are nontransparent controls, meaning that they are visible to end users. As organizations push their content-aware DLP deployments to more-advanced business-centric use cases, they are demanding the increasing automation of intelligent security decisions with a higher level of fidelity.

Better accuracy with DLP deployments yields reduced false-positive rates, reduced overall administrative workloads, reduced end-user impacts and reduced impacts to legitimate business operations. One approach to address this is to incorporate more contextual information as part of the automated DLP decision-making process itself.

Organizations, for good reasons, are typically shy about enabling automated actions (such as blocking, preventing or remediating) unless they have some level of assurance that this action will be performed in a consistent and predictable manner with a very high level of accuracy.

Better understanding the context surrounding an event leads to a more accurate decision process, which is fundamental to successful data governance and DLP.

Return to Top

Business-Context-Friendly Interfaces

Although, in the past, content-aware DLP solutions were often seen as an IT/IT security solution looking for a need, today content-aware DLP deployments are seen more and more as business tools that need to be operated and managed by the business units themselves, to address their own compliance and IP protection mandates.

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; instead, solutions need to evolve into developing reports linked to the way in which they will be used outside the IT and IT security departments.

As a result, one of the regular concerns Gartner hears from clients involves the overall complexity in using and managing content-aware DLP solutions by nontechnical staff — specifically, business process owners, information owners and other business users — who are in the rightful position to accept or reject the risks associated with the handling of their data. These users are often challenged by the traditionally technically focused administrative and event workflow interfaces offered by solution providers.

As content-aware DLP deployments continue to progress to broader business protection use cases, direct vendor offerings, along with third-party solution providers such as Bay Dynamics and others, will increase their investments in providing more business-appropriate and more easily consumable management interfaces that provide meaningful business-centric context around events.

Return to Top

Content-Aware DLP Buyer Profile

Vendors reported that the majority of content-aware DLP buyers were the office of the chief information security officer (CISO) or CIO, or, more broadly, the information security team, with funding typically originating from risk compliance or legal budgets, with a smaller proportion originating directly within IT.

The average size of buying organizations for enterprise content-aware DLP is now typically within the 3,000- to 7,000-seat range, with a sweet spot around 6,000 seats. While there are sightings of significantly larger deals — such as 50,000 and more than 100,000 seats — these larger deployments are no longer as commonplace as they used to be, due to higher market penetration within this segment.

This trend is significant because smaller organizations have a lower appetite to self-deploy and own a DLP infrastructure, resulting in an increase in interest for deployment options, such as content-aware DLP as a managed service offering.

Return to Top

Content-Aware DLP as a Managed Service

As the market for content-aware DLP grows, a more diverse ecosystem of organizations of varying sizes, market segments, know-how, maturity and technical expertise are deploying or considering deployments. While many opt to deploy and manage a content-aware DLP solution themselves, a growing number of organizations are becoming very aware of some of the more traditional deployment challenges associated with content-aware DLP.

One of the more critical deployment challenges is finding and retaining knowledgeable DLP staff that will be capable of working with the business units to create the appropriate content rules, policies and workflows; eliminate or reduce false positives; and take a leading role to address both technical and nontechnical deployment issues, including people and processes.

While organizations typically leverage professional services in the onset of a content-aware DLP deployment, many are recognizing the long-term value of the breadth and depth of accumulated experience, proven deployment methodologies and expert-level technical know-how, to more quickly address a broader set of diverse requirements in the longer term.

During the past 18 months, a significant number of organizations have inquired about the possibility of having vendors or traditional managed service providers operate a content-aware DLP deployment for them. While this does not solve the issues related to addressing internal business processes impacting their content-aware DLP deployments, it does remove the technical overhead.

Organizations surveyed by Gartner that are leveraging managed service offerings report faster time to value in their deployment versus traditional internally managed deployments. This is due, in part, to the managed service providers leveraging proven deployment methodologies as part of the day-to-day deployment, and not just at the onset, resulting in significant increases in overall deployment speed, especially when considering more-advanced deployment scenarios.

The organizations 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.

In 2013, content-aware DLP as a managed service is a nascent market with few available options; however, Gartner has identified a growing trend for vendor, solution reseller and managed service providers planning to enter this market during the next 18 months. By 2016, Gartner estimates that 20% of the deployed DLP solutions will be under the auspices of a managed service offering.

Return to Top

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 the ongoing, long-term operations of the content-aware DLP system. Specifically, the review of content-aware DLP events needs to be performed by line of business (LOB) personnel versus IT or IT security personnel, because LOB personnel are responsible for making a business decision regarding 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 an IP address or a Mac address with a username. Support for these features has become common, but they 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.

Return to Top

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 the limitations of OS APIs, variability in OS configurations, and differing computing capabilities and battery life expectations, content-aware DLP vendors do not have the interface to install 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.

Return to Top

Virtualization, Cloud and Non-Windows OS Support Are Still Lagging

The use of content-aware DLP for virtual environments has become more pronounced in the past 12 months; however, while the baseline capabilities are quite similar among the leading vendors, advanced capabilities and integration with third-party offerings vary significantly.

Some do not support the installation of their DLP solution within a virtual machine (VM), 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 with a traditional physical system, rather than providing a common high-throughput service layer available to multiple VMs concurrently.

The rate of Gartner clients inquiring about DLP integration with cloud data stores (such as Office 365, Google Docs, Box.net, Dropbox, SkyDrive and Google Drive), and about various hosted email services and SaaS, rose sharply in 2013. This is in line with the greater trend for organizations deploying these solutions. Cloud deployment of content-aware DLP solutions also should be considered at an early stage of availability, with many vendors only supporting the scanning of cloud-bound data as it leaves the internal network boundary, while others invoke a "phone home" capability — meaning that data must be pulled from the cloud environment and analyzed using appliances on-premises within the enterprise. While Gartner had expected significant development in this area during the past 12 months, based on vendors' planned road maps, the availability of solutions has been, on average, slower than anticipated.

Windows continues to be the OS of choice for support for vendors included in this Magic Quadrant. As in previous years, many vendors promised support for Apple's OS X if demand was high enough; however, it appears that current demand is still lacking. 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. Near parity of an OS X content-aware DLP agent with its Windows counterpart is still mostly a long-term road map item. As was the case last year, Gartner still 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 a few vendors, and no other vendor has any plans for this platform. Until clients make it a buying criterion to have support for OS X and Linux platforms, vendors will continue to speak of it in future terms.

Return to Top

Mainframe Integration Is All but Ignored

While clients seem interested in the notion of performing data discovery of sensitive data on the mainframe, none of the vendors evaluated in this research had plans to directly support mainframe data discovery themselves. Of those with interest, most were looking at a joint relationship with third-party organizations (such as Xbridge Systems) that have a focus on developing capabilities for scanning and analyzing mainframe data assets.

Return to Top

Gartner Inquiry Data and Observations About Content-Aware DLP

Gartner inquiry data through 2013 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 21% of all DLP inquiries — up from 12% last year, with a split of roughly 60% focused on soft IP protection (essentially, text-based assets, such as process documentation) and 40% focused on hard IP protection (such as CAD/computer-aided manufacturing [CAM] files, chemical formulas and source code).
- 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 — continues to show significant improvement in overall growth, along with the breadth and scope of deployments in IP protection and regulatory compliance.
- The trend for the Asia/Pacific region and Japan continues to be primarily focused on content-aware DLP deployments supporting IP protection; while clients in some jurisdictions (such as Australia, India and Singapore) are primarily focused on regulatory compliance mandates.
- As with 2012, in 2013, 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.
- The primary appeal of endpoint DLP continues to be the protection of IP and supporting the controlled use of locally available resources, such as USB drives, optical media recorders, and cloud storage and synch offerings (Dropbox, Box.net, SkyDrive, Google Drive and others). Concern over the potential loss of other valuable enterprise data from insider theft and accidental leakage continues to be the leading driver for endpoint deployments.
- Most content-aware DLP solutions continue to focus on text-based content in their analysis. Although there were significant capability updates by vendors for optical character recognition support, chemical formula notation support and schematic analysis, most vendors still struggle with nontext data — even when invoking fingerprinting capabilities.
- 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, dashboards or even generalized feedback relevant to this function.
- Malicious insider and well-intentioned insider threat detection is increasing in terms of client requests for DLP, as is better integration with business context awareness.
- Incumbent antivirus and endpoint protection vendors continue to lead clients' RFP shortlists.

Return to Top

The Growing Market for Channel DLP and DLP-Lite Solutions

There is a growing market trend for the adoption of DLP-enabled offerings, meaning those that integrate DLP capabilities within the various components making up an enterprise's IT ecosystem, such as Web and email gateways and firewalls, among others. Some vendors that operate directly within this market provide content-aware DLP capabilities that are quite advanced, while others support only 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:

- AppRiver
- AvePoint
- Bull
- Check Point Software Technologies
- ContentKeeper Technologies
- DeviceLock
- Identity Finder
- Microsoft
- NextLabs
- Proofpoint
- Raytheon Oakley Systems
- Sophos
- Trend Micro
- Wave Systems
- Workshare
- Xbridge Systems
- Zscaler

Return to Top