G00277564

Magic Quadrant for Enterprise Data Loss Prevention

Published: 28 January 2016

Analyst(s): Brian Reed, Neil Wynne

Enterprise DLP continues evolving to support both content-aware and context-aware capabilities, as well as support for IT security leaders to cover broader deployment use cases beyond regulatory compliance and intellectual property protection.

Strategic Planning Assumptions

By 2018, 90% of organizations will implement at least one form of integrated DLP, up from 50% today.

By 2018, less than 10% of organizations with integrated DLP will have a well-defined data security governance program in place, up from near zero today.

Market Definition/Description

Gartner defines the data loss prevention (DLP) market as those technologies that, as a core function, perform both content inspection and contextual analysis of data at rest on-premises or in cloud applications and cloud storage, in motion over the network, or in use on a managed endpoint device. DLP solutions can execute responses — ranging from simple notification to active blocking — based on policy and rules defined to address the risk of inadvertent or accidental leaks, or exposure of sensitive data outside authorized channels.

Data loss prevention technologies can be divided into two categories:

- **Enterprise 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, or soft appliances for data discovery. Leading characteristics of enterprise DLP solutions include a centralized management console, support for advanced policy definition and event management workflow. Enterprise DLP functions as a comprehensive solution to discover sensitive data within an organization and mitigate the risk of its loss at the endpoints, in storage and over the network.

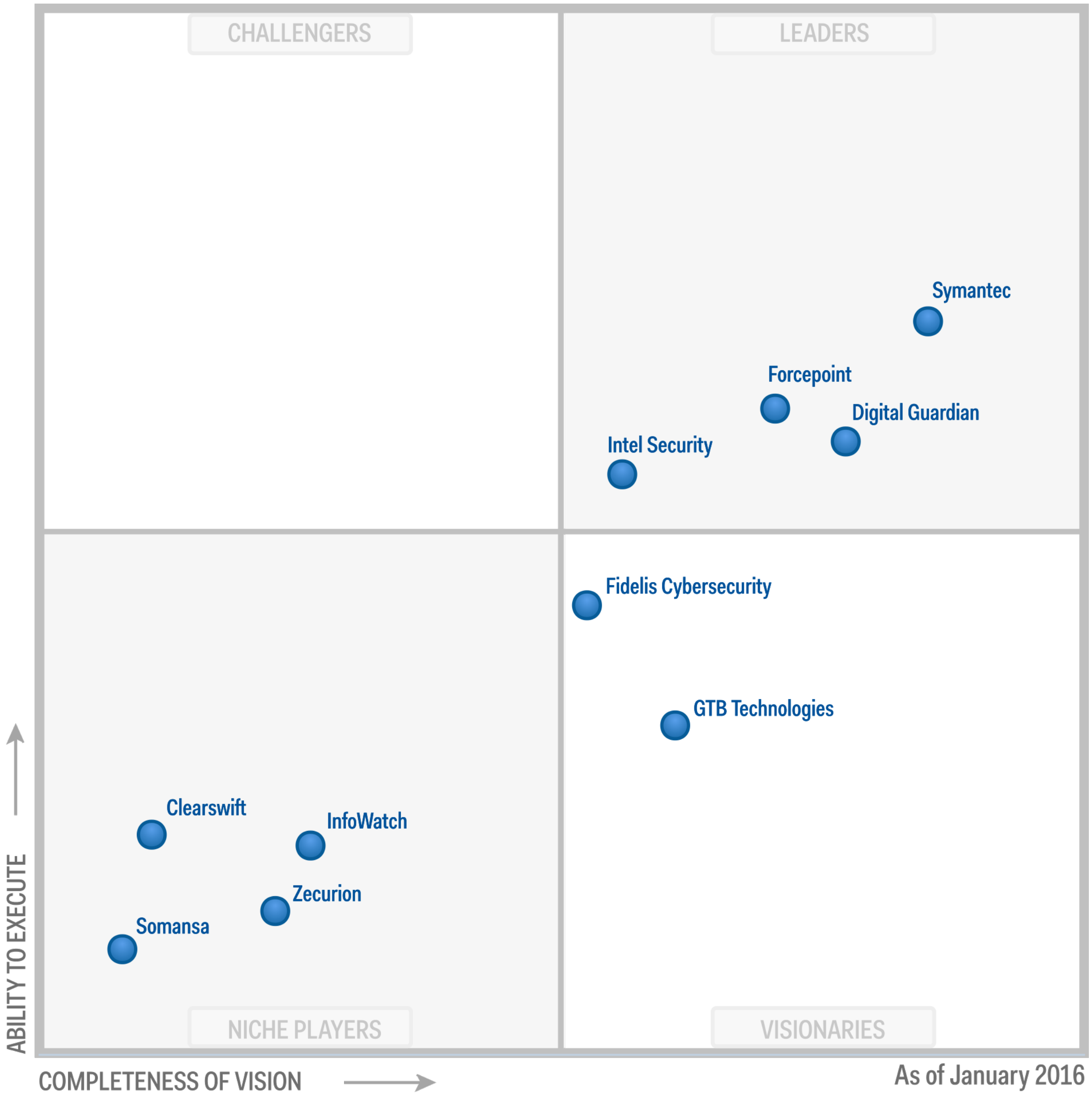
- **Integrated DLP** is a limited DLP feature set that is integrated within other data security products, including, but not limited to, secure Web gateways (SWGs), secure email gateways (SEGs), email encryption products, enterprise content management (ECM) platforms, data classification tools, data discovery tools and cloud access security brokers (CASBs). Integrated DLP usually focuses on a narrow set of regulatory compliance and basic intellectual property use cases where the data targeted for protection is easily identifiable and the policy for remediation is straightforward.

Integrated DLP will not be the primary focus of this Magic Quadrant; however, some solutions are specifically identified to highlight the differences in enterprise and integrated DLP approaches.

These updated market definitions are also defined in "Competitive Landscape: Data Loss Prevention, 2015" and "How to Choose Between Enterprise DLP and Integrated DLP Approaches."

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Data Loss Prevention



Source: Gartner (January 2016)

Vendor Strengths and Cautions

Clearswift

Clearswift is a new entrant to the enterprise DLP Magic Quadrant. Founded in 1982 and headquartered in Theale, U.K., Clearswift acquired both Jedda Systems and Microdasys for deep content and Web traffic inspection in 2013, and spent the next two years building out a fully integrated suite of adaptive DLP (A-DLP) products, brought to market in 2015.

Clearswift provides an enterprise DLP product suite that covers endpoints and servers for data-in-use and data-at-rest scanning, and data-in-motion via secure email and Web gateway controls. Common management and policy controls are managed centrally through the Critical Information Protection (CIP) Management Server. Clearswift covers multiple communication channels (email, Web and endpoint) in conjunction with centralized data security governance functionality to track and trace information movement across the enterprise.

Strengths

- Clearswift has strong network DLP capabilities and offers an "adaptive redaction" remediation option that can automatically remove inbound and outbound sensitive data while leaving the remainder of the content intact to avoid impacting business productivity.
- Clearswift's DLP management policy and reporting are centralized across its full product portfolio, including its Secure Email Gateway and Secure Web Gateway.
- Clients note favorable pricing and low complexity of deployment as key buying criteria for Clearswift's A-DLP product.
- Clearswift's data sanitization feature can remove content in file metadata, such as document properties and revision history, as well as remove active content, such as macros and embedded executables.

Cautions

- Clearswift lacks endpoint DLP support for Apple OS X and Linux operating systems.
- Data-in-motion is limited to traffic proxied through email and Web gateways.
- Clearswift's market share is low in the enterprise DLP market, as most clients recognize them for email security. DLP market presence is mainly limited to the U.K., Germany, Australia and Japan.
- Native API-based cloud support is absent. Clearswift does not offer discovery of sensitive data in the cloud within hosted email providers (Office 365, Google for Work), or within cloud storage services (Box, Dropbox, Google Drive, Microsoft OneDrive for Business, etc.).

Digital Guardian

Founded as Verdasys in 2002 and rebranded in 2014, Digital Guardian is headquartered in Waltham, Massachusetts. Digital Guardian's approach to enterprise DLP has been primarily through endpoint DLP, with strong product integration partnerships for network DLP and discovery DLP until recently. Digital Guardian acquired Code Green Networks in October 2015. Gartner received separate vendor questionnaires and supporting research information from both Code Green Networks and Digital Guardian; however, they are being evaluated as one organization.

The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux or Apple OS X, as well as support for virtual desktop infrastructure (VDI) environments.

The Code Green Networks solution covers network DLP, cloud data protection and data discovery, and is provided as a hardware appliance, soft appliance and/or virtual appliance. Digital Guardian intends to go to market with separate network and endpoint DLP solutions until product integration has been completed.

Digital Guardian has an existing partnership in place with Fidelis Cybersecurity for network DLP, the future of which will certainly be impacted by the acquisition of Code Green Networks.

Strengths

- Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux desktops and servers are supported.
- Digital Guardian has strong capabilities to support complex use cases involving intellectual property and trade secret protection via content and context awareness, as well as the forensic logging and correlation of all activities.
- Clients report faster deployment times and successful projects when utilizing both the Digital Guardian product as well as the hybrid managed security program (MSP) deployment model. The Digital Guardian Managed Security Program can be an attractive option for organizations that are seeking to outsource some (hybrid MSP) or all (full MSP) of their DLP operations.
- Digital Guardian's strategy demonstrates a strong understanding of the technology, security and jurisdictional trends that will shape its offerings going forward.

Cautions

- Digital Guardian's monitoring, discovery and control of cloud-based applications is agent-based; however, the acquisition of Code Green Networks is expected to enhance these cloud data protection capabilities with native API-based integrations to cloud storage providers such as Accellion, Box and Citrix.

- The deep OS integration of Digital Guardian's endpoint DLP agent can result in performance issues on resource-constrained systems. Proper application functionality requires more careful testing of software updates and upgrades.
- Structured data fingerprinting is not supported on the Digital Guardian endpoint agent; however, this is another gap slated to be filled by the acquisition of Code Green Networks, which currently supports data fingerprinting.
- Considerable effort will be required to effectively consolidate the Digital Guardian endpoint management features with the management capabilities that exist with Code Green Networks. The future roadmap and releases for merging these two products should be closely watched.

Fidelis Cybersecurity

Fidelis Cybersecurity was founded in 2002, acquired by General Dynamics in August 2012, and spun back out as an independent, private company through an investment by Marlin Equity Partners in 2015. Headquartered in Waltham, Massachusetts, Fidelis positions itself as an independent security company. The number of employees has grown considerably in the last year, due to bringing over several former General Dynamics employees to focus on security operations and incident response, as well as through growth from private equity investment in hiring an enterprise-focused field sales team. In addition, Fidelis acquired Resolution1 Security in May 2015, adding additional employees focused on endpoint detection and response technology. The company is poised to fulfill its vision of comprehensive advanced threat defense from network to endpoint and mobile devices.

Fidelis and Digital Guardian have a joint technology integration partnership that has been in place for several years, in which the DLP offering from Fidelis is integrated within the management console offered by Digital Guardian, providing a full-suite DLP solution. Due to Digital Guardian acquiring Code Green Networks, and Fidelis focusing on broader threat detection, Gartner anticipates Fidelis expanding beyond DLP to more broadly compete for opportunities in network security, advanced threats, and endpoint detection and response markets. Fidelis' DLP technologies will remain a core capability of the overall Fidelis XPS platform.

Strengths

- The Fidelis XPS product continues to have one of the strongest network content inspection and throughput capabilities available.
- Fidelis XPS is now offered in several models that support from 25 Mbps to 5 Gbps of throughput and beyond with the same network DLP capabilities. The smaller form factors provide a lower-cost solution to a wider market.
- 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.
- Government continues to be a significant percentage of Fidelis' customer base, bolstered by Common Criteria certification, FIPS 140-2 Level 1 compliance, along with several Authority to

Operate (ATO) and Certificate of Networthiness (CON) certifications for different classification levels on many U.S. Department of Defense networks.

Cautions

- Fidelis XPS is expensive. This can be attributed to the fact that Fidelis performs network DLP, IPS, threat intelligence, payload analysis and sandboxing all in a single product, and few customers ultimately buy Fidelis solely for stand-alone network DLP capabilities.
- Fidelis relies on a partnership with Digital Guardian to provide endpoint DLP. While Gartner does not anticipate any major changes to this partnership in 2016, this will likely change in 2017 and beyond.
- Fidelis added an endpoint agent to its portfolio with the acquisition of Resolution1, but its DLP capabilities are negligible, as it focuses primarily on EDR.
- Clients note that the Fidelis XPS CommandPost policy and rule management system is overdue for feature and user experience (UX) improvements.

Forcepoint

In 2015, Raytheon and Vista Equity Partners completed a joint venture that combines Websense (a Vista Equity portfolio company) and Raytheon Cyber products, creating a new company, now called Forcepoint. Raytheon owns a majority share of Forcepoint, while Vista Equity Partners maintains a minority interest.

Forcepoint has been considered a leader in the enterprise DLP market for several years now, previously as Websense. The AP-DATA product line is part of its Triton architecture, and includes Triton AP-Data Discover, Triton AP-Data Gateway and Triton AP-Endpoint DLP.

From years of delivering enterprise DLP, and integrated DLP modules for its secure Web and email gateway products, Forcepoint has built out a compelling enterprise DLP suite to cover network, endpoints and data discovery (both on-premises and in the cloud), with particular focus on intellectual property (IP) protection and regulatory compliance policy implementation.

Strengths

- Forcepoint supports discovering sensitive content stored in Box, Microsoft Exchange Online and Microsoft SharePoint Online using native APIs. Additionally, Forcepoint can fingerprint structured data stored in Salesforce.
- Forcepoint provides a series of predefined policies designed to identify insider threats and compromised endpoints by combining advanced content analysis and context awareness techniques.
- Forcepoint offers its enterprise DLP policy engine (Triton AP-Data) from a multitenant cloud-based infrastructure, although this is currently only available through the cloud SWG product (Triton AP-Web Cloud).

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

Cautions

- Raytheon's involvement in the defense market may help reinvigorate Forcepoint with additional intelligence and products (e.g., SureView Insider Threat); however, it is still fraught with execution risk.
- Forcepoint's relevance in some geographies will be problematic due to Raytheon's strong U.S. allegiance and federal government focus.
- Forcepoint had some notable support issues in 2014 related to the Websense corporate move from San Diego, California to Austin, Texas, but clients report generally positive feedback for DLP support in 2015. However, this is something that should be closely monitored due to changes in 2016 with Forcepoint.
- The acquisition of Intel Security's firewall business, as well as any potential new acquisitions, should be followed closely to ensure that resources are not taken off of Forcepoint's data security business.

GTB Technologies

Founded in 2004 and headquartered in Newport Beach, California, GTB Technologies' enterprise DLP suite supports network DLP, endpoint DLP, discovery DLP and information rights management.

The GTB DLP product line includes the GTB central console server (physical or virtual instance) and a single Inspector installation (either physical or virtual instance) for network DLP monitoring and enforcement. GTB Discovery performs local system, network and cloud-based discovery of data. The GTB Advanced Endpoint Protector software is available for Windows endpoints, servers and VDI environments.

Inspector looks at all ports and protocols, and performs protocol analysis to determine the type of traffic over that connection and what content needs to be inspected. The optical character recognition (OCR) server has capabilities for all DLP components, including the ability to redact partial images and identify partial or full images embedded within images or other content types. All products can be run on physical hardware or run inside of a virtual machine (VM) instance.

Strengths

- GTB's combination of data fingerprinting, OCR and native Secure Sockets Layer (SSL) decryption provides powerful interception capabilities, particularly for intellectual property protection use cases.
- GTB offers good support for discovering content within hosted email providers and cloud storage products through native API-based integrations.

- Clients report favorable pricing for the available capability set and a very positive overall experience with GTB's customer support organization.
- GTB has extensive coverage of cloud data discovery through support of Box, Dropbox, Google Drive and Microsoft OneDrive for Business.

Cautions

- GTB has low penetration in the global enterprise DLP market. GTB has been in the U.S. market since 2005, but has not advanced its DLP offerings there or in Europe. However, GTB has good penetration in Asia/Pacific (APAC), particularly Japan and Taiwan.
- GTB lacks brand recognition, so it will need to step up marketing efforts in order to expand more rapidly.
- GTB does not have a strong channel sales presence, and has a limited direct sales staff. This adversely impacts its market visibility.
- Advanced Endpoint Protector currently lacks full support for Apple OS X and Linux.

InfoWatch

InfoWatch was founded as a project by Kaspersky Lab, and has a strong market presence in Russia/Commonwealth of Independent States (CIS), as well as APAC and Latin America. Traffic Monitor focuses on looking for insider threats and risky data use by employees. InfoWatch commonly sells professional services as well as products, and can customize policy significantly based on a client's specific requirements. InfoWatch provides the evidence basis for legal hold and incident investigations, as well as robust language support for DLP policy.

While InfoWatch has been in the DLP market for several years, geographic expansion is still in its infancy and expected to continue into 2016. Client inquiries from countries outside of its installed base of Russia have been noticed, particularly in Latin America, South Asian countries and India; however, the vast majority of its revenue is from operations in Russia. The product must continue to further evolve, and global expansion will be closely monitored in 2016.

Strengths

- InfoWatch's data fingerprinting capabilities include dedicated options for scanning and detecting official documents and stamps (for example, passports and passport entry stamps).
- InfoWatch's linguistic analysis capabilities cover a broad range of languages, including those that are not typically supported in this market, such as Hindi.
- InfoWatch receives positive feedback from clients for customer experience.
- InfoWatch has made notable geographic advancement into Latin America, India and the APAC region.

Cautions

- InfoWatch's endpoint DLP agent does not have native content inspection capabilities and relies on the network component to perform these operations, which limits its use for remote endpoints.
- Native, API-based cloud support is absent. InfoWatch does not offer discovery of sensitive data in the cloud within hosted email providers or cloud storage products.
- Similar to other small vendors, InfoWatch lacks brand recognition, so it will need to step up marketing efforts and sales channel development in order to expand more rapidly.

Intel Security

McAfee was founded in 1987, acquired by Intel in 2010 and rebranded as Intel Security. The Intel Security DLP technology comes primarily from two past McAfee acquisitions — Onigma in 2006 for endpoint DLP, and Reconnex in 2008 for network and discovery DLP.

The Intel Security approach has been to integrate these acquisitions with the McAfee ePolicy Orchestrator (McAfee ePO) system for managing policy, monitoring alerts and correlating data security events between DLP events on endpoints, transmissions over the network, and data discovered at rest on file shares and repositories in the organization. The recent DLP 9.4 release brought a welcome and much-needed refresh to the endpoint DLP agent with improved policy capabilities and a redesigned DLP Discover with a smaller footprint; however, Network DLP Monitor and Network DLP Prevent need attention and focus.

Intel Security is in a state of flux with many of its security business units, most recently exiting the SEG market and selling its firewall assets to Forcepoint. Intel Security asserts that DLP remains one of its core businesses.

Strengths

- DLP integration within McAfee Web Gateway proxy supports decryption and re-encryption of Web traffic for on-the-fly content inspection, including hosted email providers and cloud storage products.
- The capture database can index and store all data seen on the network and endpoint components. Clients have reported this useful for testing new rules, forensic analysis of events that occurred prior to the creation of rules, and after-the-fact investigations. This also supports e-discovery and legal hold functionality, as well as integration directly with Guidance Software and AccessData products.
- Intel Security tightly integrates with Titus and Boldon James for data classification.
- The Security Innovation Alliance (SIA) continues to be robust, and a good way for Intel Security customers to maximize their DLP investments due to proven and tested product integrations from data classification, digital rights management (DRM), and user and entity behavior analytics (UEBA) vendors.

Cautions

- Intel Security's Enterprise DLP strategy is unclear and lacks innovation compared to its competitors. Product innovation has been largely limited to ePO integration, and network DLP product development noticeably trails the attention given to endpoint DLP.
- While the endpoint and network events can be viewed together in ePO, Network DLP Prevent and Network DLP Monitor continue to be managed separately from ePO. This is a key area of integration that should have become consistent by now, considering that the component product acquisitions occurred well over five years ago.
- Native API-based integrations with cloud storage providers is still absent. Intel Security does not offer discovery of sensitive data in the cloud within hosted email providers or cloud storage products.
- Intel Security added Apple OS X endpoint support; however, this currently provides only device control, rather than the full DLP capabilities available through the Windows agent. Linux is not supported.

Somansa

Somansa is a new entrant to the 2016 enterprise DLP Magic Quadrant. The company was founded in 1997 and first released its network data loss detection (DLD) products in 1999. Somansa has a strong APAC presence, and considerable operations located in its main headquarters of Seoul, South Korea. Somansa has all three major components of an enterprise DLP solution — Privacy-i for endpoint DLP and discovery DLP, and Mail-i for network DLP, supporting email, HTTP/HTTPS, instant messaging and FTP protocols. Both of these products had updates in mid-2015.

Somansa has a notable presence in the government sector outside of the U.S., particularly in the APAC region. It also has clients in Latin America, the U.S. and Canada, and has operations in San Jose, California to provide North American support. Somansa's presence in Europe is relatively small, with a few key business partners.

Strengths

- Somansa supports discovering sensitive data stored in Amazon S3, Box, Dropbox, Microsoft OneDrive, Microsoft Office 365, Salesforce and Google Drive using native APIs.
- Customers have very positive feedback about Somansa's support and rapid resolution of issues, particularly in providing patch updates.
- Somansa supports regulatory and compliance mandates specific to the Asia/Pacific region through predefined policies and delegated administration to upper/department management for quarantine review and release.
- Somansa has support for Discovery DLP within CRM and ERP applications, and supports a wide range of platforms and data types.

Cautions

- Somansa does not support detection capabilities for partial document matching or unstructured data fingerprinting.
- Somansa's geographic reach predominantly consists of South Korea, with some deployments in Brazil, China, Japan, Mexico, Canada and the United States.
- Similar to other small vendors, Somansa lacks brand recognition, so it will need to step up marketing efforts and sales channel development in order to expand more rapidly.
- Language support for the policy engine is limited to English, Chinese, Spanish, Korean, Japanese and Portuguese.

Symantec

Headquartered in Mountain View, California, Symantec has been in the data loss prevention market since its acquisition of Vontu in 2007. In June 2015, Symantec released its Symantec Data Loss Prevention 14.0, and has product components for DLP Enforce Platform, IT Analytics for DLP, Cloud Storage (supporting Box and Microsoft SharePoint Online), Cloud Prevent for Microsoft Office 365, DLP for Endpoint, DLP for Mobile, DLP for Network and DLP for Storage. Symantec also has DLP API support for third-party security technologies, such as content extraction, reporting and FlexResponse for encrypting content or applying DRM. Despite the corporate turmoil and management turnover at Symantec over the last several years, it has remained focused on data security — specifically DLP technology — and has continued to invest and improve the DLP technology in its information protection business unit.

Strengths

- Symantec offers the most comprehensive sensitive data detection techniques in the market, with advanced functionality that can cover a wide breadth of data loss scenarios.
- Symantec supports a hybrid deployment model for several of its DLP products, in which detection servers deployed to Amazon Web Services, Microsoft Azure or Rackspace connect to an on-premises Enforce Server.
- Symantec's strategy demonstrates a strong understanding of the technology, socioeconomic, security and jurisdictional trends that will shape its offerings going forward.
- Although not functionally equivalent to the Windows endpoint agent, Symantec added Apple OS X support for basic local data discovery and remediation options, as well as exact document matching as an advanced detection option. An endpoint agent for Linux is not available.

Cautions

- Symantec's monitoring and discovery of sensitive data in cloud applications is endpoint-based, with the exception of Box and Microsoft SharePoint Online, which leverages a native API-based integration.

- Partial document matching and structured data fingerprinting are not evaluated locally on the endpoint agent; these require a "phone home" capability to the Symantec Endpoint server for analysis.
- Clients express concern with the overall deployment complexity and cost of Symantec's solution, when compared with competing solutions.
- Symantec is nearing the completion of the divestiture of Veritas and will be in a strong position to make security acquisitions both within and outside of its information protection business unit. Acquisitions not focused on information protection could serve as a distraction, delaying product roadmap items and new releases.

Zecurion

Zecurion offers enterprise DLP through Zlock (endpoint), Zgate for network DLP and Zdiscovery for data-at-rest scanning, as well as Mobile DLP for iOS and Android devices. While based in Moscow, Russia, Zecurion does have a presence in the U.S., with an office in New York City.

Similar to other regionally focused vendors, client inquiries from countries outside of its installed base of Russia have been noticed. However, the vast majority of its revenue is from operations in Russia. However, references for this Magic Quadrant included Zecurion customers in the U.S. and Latin America. In 2016, Zecurion will likely look to continue its geographic expansion plans into the APAC and Latin American markets.

Strengths

- Zecurion provides full archiving of all data seen by the endpoint agent and can also capture screen shots.
- Zecurion includes an OCR capability for identifying content.
- Zgate for network DLP controls over 250 different social media services, including LinkedIn, Facebook, Google+ and Yahoo, as well as supporting services to these sites, such as IM, Web mail and file hosting.
- Zecurion receives positive feedback from clients for pricing and customer experience.
- Language support is robust, with support for English, Russian, Czech, Slovak, Greek, German, Spanish, French, Italian, Arabic, Turkish, Malaysian, Korean and Hindi, among other regional and localized dialects.

Cautions

- Zecurion has very low penetration in the global enterprise DLP market, with the vast majority of its clients in Russia. Despite establishing an office and relationships with key resellers in the U.S., Zecurion has not advanced its DLP offerings there.

- Zlock Endpoint DLP Agent supports Windows, has limited DLP capabilities for Mac OS X, and does not support Linux.
- Native API-based cloud support is lacking. Zecurion does not offer discovery of sensitive data in the cloud within hosted email providers or cloud storage products.
- Zecurion does not offer self-remediation or user justification as remediation action options.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Clearswift and Somansa are new to the Magic Quadrant this year. Digital Guardian (formerly Verdasys), Intel Security (formerly McAfee) and Forcepoint (formerly Websense) were added due to name changes and acquisitions.

Dropped

- Absolute Software, CA Technologies and Trustwave no longer meet the inclusion criteria for this Magic Quadrant.
- Code Green Networks (acquired by Digital Guardian), McAfee (now Intel Security) and Websense (now Forcepoint) were dropped due to name changes and acquisitions.
- EMC (RSA) has been dropped due to its announcement of the end-of-life status of their DLP product business. See the section below specifically about EMC's exit from the DLP market.

Inclusion and Exclusion Criteria

Inclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

The following vendor attributes are required to qualify for inclusion:

- $8 million in annual revenue specifically for their enterprise DLP product(s).
- Ability to detect sensitive content in network traffic without the need for an endpoint agent.
- Ability to detect sensitive content in either discovery scans (data at rest) or endpoint (data in use).

  - Solutions that can solve for all three scenarios of network, endpoint and data discovery will be viewed as more complete.
- 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.
- Generally available as of 30 September 2015.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.

Exclusion Criteria

Vendors are excluded from this Magic Quadrant if they meet the following criteria:

- Solutions that depend upon integration into another product, including but not limited to an email server, secure email gateway or secure Web gateway
- Solutions that do not have a single centralized management interface and event workflow repository for discovery, endpoint and network DLP
- Solutions that use only simple data detection mechanisms (for example, supporting only keyword matching, lexicons or simple regular expressions)
- Solutions with network-based functions that support fewer than four protocols (for example, only SMTP email, FTP and HTTP)
- Solutions that primarily support DLP policy enforcement via content tags assigned to objects
- Solutions that cannot detect sensitive content accessed over the network without requiring DLP endpoint software installed
  - Specifically, the ability to detect data in motion to unmanaged systems or devices

Please note that vendors with minimal or negligible apparent market share among Gartner clients, or with no current generally available services, may be excluded from this Magic Quadrant.

Evaluation Criteria

Ability to Execute

Ability to Execute is ranked according to a vendor's ability to provide the market with an enterprise 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 enterprise DLP technology capability. This is the most exhaustive of all of the assessed criteria.
- **Overall Viability** assesses the organizational health of a vendor, taking into account its ability to execute on a strategy and significantly grow its business. In a maturing market moving toward mainstream, this evaluation criterion was added to this update of the DLP Magic Quadrant.
- **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 roadmaps, the content of future product roadmaps and the cultivation of strategic advantages.
- **Marketing Execution** is new to this Magic Quadrant, and measures how vendors are marketing their solutions in order to grow their customer base in specific demographics.
- **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, including support across data silos, different operating systems and content types.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (January 2016)

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 enterprise 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 organizations' 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, data 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, roadmaps 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.
- **Business Model** assesses the overall go-to-market strategy of a vendor, its current product portfolio, past performance and future plans for expansion, and its overall business conditions. This evaluation criterion was newly added to this update of the enterprise DLP Magic Quadrant.
- **Vertical/Industry Strategy** examines specific features, functionality and go-to-market strategy that focus on specific segments of the market or industry vertical, in order to gain competitive advantage and gain customers. This evaluation criterion was newly added to this update of the enterprise DLP Magic Quadrant.
- **Innovation** looks at the innovative features that vendors have developed, to assess whether the vendors are thought leaders or simply following the pack, and 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	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (January 2016)

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 meaningful integrations. They offer aggressive roadmaps and usually deliver on them. Their DLP products are well-known to clients and are frequently found on RFP shortlists.

Challengers

Challengers have more competitive visibility and execution success in specific mature industry sectors than Niche Players. Challengers offer all the core features of enterprise DLP, but typically their vision, roadmaps and/or product delivery are narrower than those of Leaders. Challengers may have difficulty communicating or delivering on their vision in a competitive way outside their core industry sectors.

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.

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 geographic reach, functions and platforms — or when 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 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).

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 organization's data security needs and budget. Every organization should consider DLP as part of its information security management program. DLP capabilities come from a variety of different types of products — both cloud-hosted and on-premises. The main theme remains that DLP is ultimately a well-defined data security process, bolstered by well-managed supporting technology.

Market Overview

Data loss prevention and the enterprise DLP market are currently experiencing a renaissance through a "second wave" of adoption. As noted on the "Hype Cycle for Data Security, 2015," data loss prevention has clearly moved to the right of the Trough of Disillusionment and climbing toward the Plateau of Productivity. There have been a number of reasons that this has taken place in the last two years.

First, look no further than the breach activity that has engulfed organizations in nearly every sector of the global economy. While DLP is not designed to stop data theft in every conceivable scenario (and was never intended to do so), DLP technology can provide a key element of data visibility when used in concert with other detect and respond technologies. Few data security controls delineate between either motivated insiders or users who unknowingly exfiltrate sensitive data. This has provided an environment where organizations are left scrambling for security tools that can provide any additional visibility and context to aid in the detection of and response to data security incidents.

The first wave of DLP adoption that drove the market into the Trough of Disillusionment focused on DLP as a data security "silver bullet." It was often billed as a way to identify and stop every case of accidental data loss and purposeful data theft. The market has since matured and evolved. Vendors and customers have become aware that enterprise DLP is a key piece of a broader and larger data life cycle process supported by technology, as opposed to DLP simply being another technology buying decision.

EMC's RSA Data Loss Prevention Suite End-of-Life Announcement

EMC's RSA Data Loss Prevention Suite has been a mainstay product in the DLP market since the acquisition of Tablus by RSA in 2007. In the beginning of 2015, EMC began notifying customers that it considered its DLP 9.6 release to be "feature complete," and would not be continuing development with any new or updated product releases. This covers the entire RSA DLP suite of products — DLP Datacenter, DLP Network and DLP Endpoint. EMC has discontinued forward investment in DLP, and those resources have been reallocated to products such as RSA Security Analytics, which EMC believes better addresses organizations' ability to detect and respond to data breaches.

The exit of RSA DLP has been a significant source of Gartner client inquiries related to DLP in 2015. We have been tracking these calls, and approximately 10% of all calls related to data loss prevention from April 2015 to December 2015 have been about the RSA DLP end-of-life announcement and plans by Gartner clients to migrate to a different enterprise DLP vendor.

According to the end of product support (EOPS) information from EMC (available at emc.com), clients currently on RSA DLP 9.5 can extend support for one year (through November 2016). Gartner recommends all current RSA DLP customers be sure to upgrade to version 9.6 as soon as possible, which will reach EOPS status in December 2017, with the option to extend support for one additional year through December 2018. This should provide ample time for clients to carefully evaluate whether they should replace RSA DLP with a comparable enterprise DLP vendor, or look at an integrated DLP approach with multiple vendors and products, which might provide greater data visibility and use-case coverage.

RSA DLP also impacts other businesses. The Cisco Email Security Appliance (ESA) product business has integrated the RSA DLP engine in the email security platform. This caution was noted on the most recent "Magic Quadrant for Secure Email Gateways" and warrants mention again.

At this point, there are multiple possibilities for the RSA DLP technology. It could simply reach end-of-life status and not be developed further. EMC might also choose to sell this technology to another vendor, although the chance of this has decreased since it has already announced end-of-life plans and customers are making active migration plans away from RSA DLP. Still, the possibility for the technology to live on or be delivered to market in another way still exists.

Enterprise DLP Versus Integrated DLP

Data loss prevention capabilities are integrated into a wide variety of security point products. IT leaders struggle to understand the depth and breadth of integrated DLP capabilities, their appropriate intended use cases, and when to implement these technologies and/or "best-of-breed" enterprise DLP products.

As noted above in the Market Definition, enterprise DLP and integrated DLP can each play a pivotal role in an overall data life cycle protection strategy for your organization. They are also not mutually exclusive. As an example, organizations may choose to enable DLP capabilities at the secure email gateway, secure Web gateway and cloud access security broker, and choose not to deploy network DLP. Some organizations may not have the ability to strictly control endpoint systems; therefore, other technologies must be employed to provide visibility into data movement and data usage. Organizations should not limit their view of valid DLP solutions to only enterprise DLP products. Integrated DLP will result in many distinct policies across separate security controls, and without a proper policy management strategy, it is doomed to failure.

Both enterprise DLP and integrated DLP must provide content-aware and context-aware capabilities to be reasonably effective. Please refer to "How to Choose Between Enterprise DLP and Integrated DLP Approaches" for further information.

Microsoft and Its Impact on the DLP Market

Microsoft made a significant push into multiple information security markets in 2015. It added native DLP capabilities throughout its Exchange, SharePoint and OneDrive for Business platforms, both on-premises and online. Natively, Microsoft has included some key security capabilities (see "How to Enhance the Security of Office 365") — and specifically, DLP capabilities (see "Data Loss Prevention in Microsoft Office 365").

Microsoft has also made two noteworthy acquisitions in 2015:

- **Adallom —** A CASB that provides visibility, compliance, data security and threat prevention capabilities between end users and cloud applications/storage. Adallom was acquired by Microsoft in September 2015.
- **Secure Islands —** A data classification and tagging solution that allows users to identify and tag sensitive content, and also allows for integrated DLP actions to be taken based upon the tag value (for example, add rights management to an Excel file tagged as "Financial Data"). Secure Islands was acquired by Microsoft in November 2015.

Many of the enterprise DLP and integrated DLP vendors have also stepped up with product enhancements (or strategic partnerships) that add DLP support for both Microsoft Office 365 and OneDrive for Business, as these are key applications for organizations moving from on-premises infrastructure and applications to infrastructure as a service (IaaS) and SaaS.

Data Classification and Tagging Complementary to DLP

Data classification and tagging has been identified as a capability for file analysis software, as noted in "Market Guide for File Analysis Software." Data classification and tagging, in a security context, typically include the capabilities to both apply a metadata tag or value to unstructured or semistructured content, and take some form of data action based on the tag value, including encrypt, apply digital rights management or block transmission.

Gartner clients note three main drivers for data classification and tagging projects:

1. **Data classification and tagging used in conjunction with an enterprise DLP product —** Many of the enterprise DLP products covered in this Magic Quadrant have the ability to identify, create and set DLP policy rules based on the existence of metadata values or tags attached to a file. This is commonly used in enterprise DLP policy as an additional screening layer to aid in reduction of false positives on content inspection rules and add additional content controls. This is most commonly used to apply encryption or electronic digital rights management (EDRM) based on a metadata value or tag.
2. **Data classification employed as a stand-alone system for classifying content scanned in a data-at-rest project —** These efforts center on data classification and data life cycle management, with goals to identify where sensitive data is stored on-premises in file shares or content management systems, as well as online in cloud storage platforms. These efforts are particularly useful to tag data that has not been accessed for a certain time period, or has a certain type of sensitive data or a number of sensitive records. This can be valuable in identifying data suitable for archiving or deletion, which is further along the data life cycle.
3. **Data classification used as a means to address the mobile data use case —** An example is sensitive data moved to an unmanaged asset where a DLP endpoint is either not deployed (or cannot be deployed), such as a tablet or phone, yet there is still a need to retain security

controls or tag values of a specific file or data type. Frequently, this is tied to deployment of EDRM, such as Microsoft Azure Rights Management Service (RMS).

Data classification products typically have two main classification capabilities:

1. Automated classification based upon content libraries, rules, heuristics and Bayesian classifiers and other content string identification systems.
2. User-driven classification that empowers users to apply initial content tags to unstructured content at either the time of creation or editing; that content tag can either persist through the life of that data, or can be edited or appended by other users.

There are pros and cons to either data classification approach. With automated classification, you start with a programmatically driven decision about data, and your tags will only be as intelligent or sophisticated as the classification policy and engine allow. User-driven classification allows data owners and content creators who are closest to the data to self-identify and establish data tags. The major drawbacks are human error and reliance on data owners to be savvy about the types of data they access, and making judgments calls such as "confidential" versus "highly confidential." For further guidelines on data classification in the context of data security, please see "How to Overcome Pitfalls in Data Classification Initiatives."

DLP Managed Services

DLP managed services have dramatically increased in both popularity and adoption in the last two years. Thirteen percent of all Gartner client inquiries for data loss prevention in 2015 mentioned DLP as a managed services offering.

DLP managed services are different from MSSP for other security technologies, such as firewalls or intrusion prevention systems, where the primary focus is log management. DLP managed services depend on a proper implementation, and a thorough understanding of the policy and rules, to optimize event workflows and to understand serious data security issues from noisy events.

The same vendors that are traditionally strong in the MSSP market do not always carry over that same strength to managing DLP. DLP requires a considerably different approach to managing the event workflow — it's not a volume game, or even one aided considerably by event correlation. Understanding both asset criticality and data criticality from data owners are two key elements to having a successful DLP managed services offering. DLP systems are not always something that you want to allow third-party access to — or hosting of, in some cases — especially for clients with strong data residency concerns.

Symantec and Digital Guardian are two vendors most frequently mentioned by clients looking for a managed services option. Symantec has a strong network of partners that manage all of the components of the Symantec DLP product suite. InteliSecure, infoLock Technologies, Novacoast and Wipro are commonly mentioned as implementation partners that can both implement Symantec DLP and provide DLP managed services. Digital Guardian has its own MSP approach that allows customers to choose flexible deployment options, and choose for either Digital Guardian to host the DLP management infrastructure, or for the customer to retain hosting on-premises in the organization. Forcepoint, Intel Security, Fidelis Cybersecurity and GTB Technologies also have partnerships for DLP managed services; however, those vendors appear less frequently among Gartner clients. Raytheon's acquisition of Foreground Security in October 2015 will likely improve Forcepoint DLP managed services, particularly for U.S. federal government clients.

Strongly consider DLP vendors that have management platform flexibility (cloud, hybrid or on-premises), as well as flexible deployment options for endpoint and network DLP. Also look for those DLP managed service providers with vendor-certified security analysts on staff, current client references and a proven track record of helping organizations improve the operational workflow of DLP implementations into actionable and usable information.

Intersections Between DCAP and DLP

Data-centric audit and protection (DCAP) is a category of products characterized by the ability to centrally manage data security policies and controls across unstructured, semistructured and structured repositories or silos. Based upon data security governance (DSG) principles, these products encompass the ability to classify and discover sensitive datasets and control access to the sensitive data by centrally managing and monitoring privileges and activity of users and administrators.

There is a critical need to establish organizationwide data security policies and controls based upon DSG. DSG allows an organization to achieve a balance between appropriate security and competitive advantage by classifying and prioritizing security and expenditure for particular sensitive datasets. Each dataset has its own protection, storage and controls that will vary as a function of time (for example, sales, intellectual property and personally identifiable information [PII] datasets have different lifetimes). By using the DSG process to engage key stakeholders (such as business, IT, governance, compliance/legal and risk), organizations can then approve whether each dataset merits investment in security controls that mitigate particular risks associated with compliance or data threats, or to protect intellectual property. There are many data security products available, each with different security control capabilities, but most focus on particular data silos (see "Market Guide for Data-Centric Audit and Protection"). The challenge facing organizations today is that data is pervasive and does not stay in a single silo on-premises, but is compounded by the use of cloud SaaS or IaaS. Organizations must apply DSG before implementing any data security product or process.

DSG drives data classification and discovery to be core requirements for many data security products, including DCAP and DLP. DLP provides visibility into sensitive data in use on the endpoint, in motion over the network and at rest on file shares. DLP policies provide real-time protection of unstructured data being extracted from endpoints or via email. This is complementary to DCAP, which uses data classification and discovery to help with the real-time user activity monitoring of data at rest and in use within structured or unstructured silos, and the application of protective products. In cloud SaaS, data protection offerings are becoming a "melting pot" of separate DLP and DCAP policies, driving the need for data security policy orchestration between all of the silos of data security controls in an organization.

Data Loss Prevention for Cloud and Mobile Users

Data loss prevention is a necessary component of cloud and mobile computing. The way that DLP is currently implemented for cloud and mobile use cases is through the use of native data security controls within a CASB, enterprise DLP policy integration with a CASB, or application isolation or containers on managed mobile devices, such as tablets and phones.

Historically, DLP for mobile devices was accomplished through backhauling all managed device traffic through a VPN and network DLP appliance (usually limited to Web and email traffic). Cloud applications and cloud storage platforms break this model, as highlighted in "Overcome the Limitations of DLP for Mobile Devices."

DLP functionality for unmanaged devices is today best-suited to implementation via a CASB or cloud security service. Due to privacy and mobile device constraints, having a useful mobile agent on a device you do not own is simply not a reality for many users or organizations. In particular, there are not full-featured DLP agents for iPads, iPhones or the near infinite variations of Android devices that perform DLP capabilities. Most of these solutions are little more than trusted viewing agents or ways to access files shared through mobile content management (MCM). There likely never will be a DLP agent for mobile form factors, due to device limitations and resource-heavy requirements that full content-aware inspection would bring to a mobile device. For further details on mobile data protection, please refer to the "Magic Quadrant for Enterprise Mobility Management Suites."

Gartner Recommended Reading

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

"Data Loss Prevention in Microsoft Office 365"

"Overcome the Limitations of DLP for Mobile Devices"

"How to Choose Between Enterprise DLP and Integrated DLP Approaches"

"Anticipating and Overcoming the Five Key Obstacles to Success in Enterprise DLP Deployments"

"Market Guide for Cloud Access Security Brokers"

"Market Guide for Data-Centric Audit and Protection"

"Market Guide for User Entity Behavior Analytics"

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

Evidence

- Vendor surveys and recorded product demos from all vendors represented in this Magic Quadrant

- 300+ Gartner client inquiry calls centered on data loss prevention from March 2015 to January 2016
- Customer reference surveys — delivered in an online survey to 48 customers, and live interviews with 10 customers of vendors represented in the Magic Quadrant
- Gartner Secondary Research used to research company financials and market-size metrics

Evaluation Criteria Definitions

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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp