# Magic Quadrant for Enterprise Data Loss Prevention

**Published:** 16 February 2017 **ID:** G00300911

**Analyst(s):** Brian Reed, Deborah Kish

## Summary

Security and risk management leaders purchase on-premises enterprise DLP to solve for either organizationwide regulatory compliance or to better protect specific types of intellectual property, while monitoring emerging cloud DLP capabilities.

## Strategic Planning Assumptions

By 2022, 60% of organizations will involve line-of-business owners when crafting their data loss prevention (DLP) strategy, up from 15% today.

By 2020, 85% of organizations will implement at least one form of integrated DLP, up from 50% today.

By 2022, a majority of DLP market revenue will be driven by integrated DLP products, as opposed to enterprise DLP systems.

## Market Definition/Description

Gartner defines the DLP market as those technologies that, as a core function, provide remediation for data loss based on both content inspection and contextual analysis of data:

- At rest on-premises, or in cloud applications and cloud storage
- In motion over the network
- In use on a managed endpoint device.

DLP products 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.

DLP technologies can be divided into two separate categories:

- Enterprise DLP products incorporate sophisticated detection techniques to help organizations address their most critical data protection requirements. Products 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 products include a centralized management console, support for advanced policy definition, event management workflow and reporting. Enterprise DLP functions as a comprehensive system 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 products offer a limited DLP feature set that is integrated within other security products including, but not limited to, secure web gateways (SWGs), secure email gateways (SEGs), enterprise network firewalls (ENFW), intrusion detection and prevention systems (IDPSs),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 products are specifically identified to highlight the differences between enterprise and integrated DLP approaches.

## Magic Quadrant

**Figure 1.** Magic Quadrant for Enterprise Data Loss Prevention

*Source: Gartner (February 2017)*

**Vendor Strengths and Cautions**

## Clearswift

Clearswift was founded in 1982 and is headquartered in Theale, U.K. Clearswift acquired both Jedda Systems and Microdasys for endpoint 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. As of January 2017, Clearswift has been acquired by Ruag and will be part of its Defence Cyber Security business unit.

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 any product, including the gateways and Critical Information Protection (CIP) server, utilizing a common policy across all communication channels. Clearswift covers multiple communications channels (email, web and endpoint), in conjunction with centralized data security governance functionality, to track and trace information movement across the enterprise. Clearswift is a suitable choice for organizations looking to increase their email DLP capabilities.

**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 policy rules are built with an intuitive flow that asks what you want to do, presenting drill-downs for additional options.

Clearswift has a built-in data classification system that is highly tunable and also has "confidence" levels of classification that can be configured. Third-party data classification from Titus and Boldon James is also supported.

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**

It is unclear as to the direction and roadmap postacquisition by Ruag, and how it will integrate Clearswift into the overall portfolio.

Clearswift lacks endpoint DLP support for Mac OS X and Linux operating systems.

Clearswift's market share is low in the enterprise DLP market, as most clients recognize it for email security. DLP market presence is limited to the U.K., Germany, Australia and Japan.

Native cloud support is still lacking. Cloud data discovery requires a mapped drive letter in Windows to a cloud storage repository such as Dropbox or Microsoft OneDrive. However, Clearswift does have a partnership in place with GeoLang to address this concern.

## CoSoSys

CoSoSys is a new entrant to the enterprise DLP Magic Quadrant this year, and was founded in 2004 in Romania. The vendor has a global presence, with offices in Germany, South Korea, United Arab Emirates and the U.S.

CoSoSys is known for its endpoint DLP product, Endpoint Protector; however, it has also brought network DLP and e-discovery products to market as part of its overall enterprise data loss prevention product portfolio. CoSoSys also offers encryption products, mobile device management for iOS and Android, and specific DLP products that cover Linux, Mac OS X, printers, terminal servers and other virtual desktop infrastructure (VDI) thin clients. CoSoSys is a suitable choice for organizations with a wide variety of endpoint devices and the need for granular DLP policies based on operating systems.

**STRENGTHS**

CoSoSys has a wide variety of endpoint DLP platform support, with support for all versions of Windows, Mac OS X and Linux.

The CoSoSys management platform is very intuitive and easy to navigate, and clients report that monitoring and reporting are both very easy to configure and use.

CoSoSys has strong out-of-the-box support for Linux, with endpoint DLP support for CentOS, Red Hat Enterprise Linux and Ubuntu, as well as the ability to customize Linux support on a specific kernel and operating system version on request.

Customers reported that response times for technical support are favorable and that the vendor gets issues resolved quickly.

**CAUTIONS**

CoSoSys does not have strong market recognition of its network DLP or discovery capabilities.

CoSoSys redaction support is limited to text only, with no ability to redact sensitive data in PDFs or Microsoft Office document types.

CoSoSys lacks integration with third-party encryption or rights management products as remediation options.

CoSoSys is limited to agent-based DLP discovery only.

## Digital Guardian

Founded in 2002, Digital Guardian (formerly Verdasys) 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 October 2015, when it acquired Code Green Networks (CGN). It has since launched that as the Digital Guardian Network DLP product line.

The Digital Guardian endpoint covers DLP, advanced threat protection, and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux and Mac OS X, as well as support for VDI environments.

The Digital Guardian Network DLP and Digital Guardian for Data Discovery products cover network DLP, cloud data protection and data discovery, and are offered as a hardware appliance, soft appliance and/or virtual appliance. Digital Guardian worked to streamline and integrate the management capabilities among its endpoint DLP and assets from the CGN acquisition throughout 2016. Digital Guardian also has an existing partnership with Fidelis Cybersecurity for network DLP. Few Gartner clients have discussed this partnership recently, and Gartner believes that, except for existing joint clients, the partnership will continue to diminish and eventually go away entirely. Digital Guardian is a suitable choice for organizations with strong regulatory

compliance concerns, specifically in the healthcare and financial services industries, as well as organizations with intellectual property protection requirements. Digital Guardian is also a strong choice for organizations requiring uniform DLP rules to work equally well across Windows, Mac OS X and Linux operating systems.

**STRENGTHS**

Clients report faster deployment times and successful projects when utilizing the Digital Guardian product in conjunction with Digital Guardian Managed Services.

Digital Guardian has integrations with broader security products, including threat intelligence, network sandbox, user and entity behavior analytics (UEBA), cloud data protection, and security information and event management (SIEM; including apps available in the IBM QRadar and Splunk app stores).

Clients like the modular licensing for DLP endpoint, with support for Windows, Mac OS X and Linux, and endpoint capabilities that can be licensed in any combination of device visibility and control, DLP, and advanced threat protection.

Digital Guardian's vision demonstrates a strong understanding of the technology, security, threat landscape and industry trends that will shape its offerings going forward.

**CAUTIONS**

Digital Guardian lacks a common policy across the endpoint and network products.

The Digital Guardian agent cannot discern between personal and enterprise accounts for Microsoft OneDrive; however, it can prevent the use of the personal Microsoft OneDrive application.

Customers expressed concern with the integration speed of the CGN acquisition.

Structured data fingerprinting is not supported on the Digital Guardian endpoint agent, but this functionality is available via the CGN agent.

## 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. The vendor is headquartered in Washington, DC. It positions itself as an independent security company and the number of employees has grown considerably in the last year, due to bringing over several former General Dynamics employees, specifically focused on security operations and incident response, as well as through growth from private equity investment in hiring an enterprise-focused field sales team. In May 2015, Fidelis acquired Resolution1 Security, adding more employees focused on EDR technology.

Fidelis and Digital Guardian have a joint technology integration partnership, which 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 building out its own Network DLP product line, and Fidelis focusing on broader threat prevention and detection, the partnership between Digital Guardian and Fidelis has already been de-emphasized by both companies and will eventually dissolve altogether. This makes sense because buyers have long regarded Fidelis as more than a stand-alone network DLP vendor. However, Fidelis' DLP technology will remain a core capability of the overall Fidelis Network platform.

Fidelis is a suitable choice for organizations that want DLP capabilities as part of a larger platform for network threat detection and prevention, and want to buy these capabilities along with network IDPS, payload analysis, malware sandboxing and threat intelligence.

**STRENGTHS**

The Fidelis Network product continues to have one of the strongest network content inspection and throughput capabilities available.

Fidelis Network's ability to actively prevent data leaks natively, without requiring a third-party proxy, is a differentiator that appeals to its customer base.

In the last year, Fidelis introduced a hosted service offering where it hosts the management, metadata and analytics components in a managed cloud infrastructure. Fidelis Network supports deployment in either Amazon Web Services (AWS) or Microsoft Azure infrastructures.

Out-of-the-box rule sets have received positive feedback from customers.

Fidelis' customer support response times have been favorable according to customer feedback.

**CAUTIONS**

Fidelis has deemphasized DLP over the last several years, instead choosing to focus on threat prevention and EDR capabilities, creating the perception that DLP technology is less important than other capabilities offered by the vendor.

Without the partnership with Digital Guardian, Fidelis will not meet the likely future requirements for the enterprise DLP market unless it renews the partnership, finds a new technology partner, or builds out its own endpoint DLP and discovery DLP capabilities.

Fidelis' GUI has been cited as being "clunky" and for it being difficult to identify where and what rule is applied.

## Forcepoint

In 2015, Raytheon and Vista Equity Partners completed a joint venture that combines Websense, a Vista Equity portfolio company, and Raytheon Cyber Products. In 2016, the company acquired two firewall product lines from Intel Security — Stonesoft and Sidewinder — and relaunched the combined company as Forcepoint. Raytheon owns a majority share of Forcepoint, while Vista Equity Partners maintains a minority interest.

Based in Austin, Texas, Forcepoint has been considered a leader in the enterprise DLP market for several years now, previously as Raytheon-Websense. The Forcepoint DLP product line includes Forcepoint DLP Discover, Forcepoint DLP Gateway, Forcepoint Cloud Applications, and Forcepoint DLP Endpoint. In February 2017, Forcepoint announced the intent to acquire the Skyfence cloud access security broker (CASB) business from Imperva.

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 a particular focus on intellectual property protection and regulatory compliance policy implementation.

Forcepoint is a suitable choice for organizations with both regulatory compliance and intellectual property protection requirements, or for organizations that want to deploy DLP virtual appliances within the Azure public cloud infrastructure.

**STRENGTHS**

Forcepoint DLP Endpoint can automatically encrypt/decrypt files via Microsoft RMS without removing RMS protections based on endpoint data in use, data in motion and discovery rules.

Forcepoint offers its enterprise DLP policy engine from a multitenant cloud-based infrastructure.

Forcepoint provides over 350 predefined policies and an embedded UEBA component for additional security analytics features that perform incident risk ranking, identify insider threats, highlight compromised endpoints and calculate data theft risk indicators to identify the riskiest users and activities.

Structured data fingerprinting, particularly support for data fingerprinting in Salesforce, is cited by clients as a key differentiator.

**CAUTIONS**

Clients have reported technical support issues related to structured data fingerprinting. If you require structured data fingerprinting of data in a database, ensure that you thoroughly test this capability with live data in your specific database environment.

Raytheon's involvement in the defense market will help reinvigorate Forcepoint with additional intelligence and products. However, there is not a successful track record of security vendors owned by defense contractors parlaying that success into commercial markets.

Forcepoint's relevance in some geographies may be problematic due to Raytheon's strong U.S. allegiance and federal government focus. Some Gartner clients have noted this objection, and you should check whether this is a cause for concern in your organization.

## GTB Technologies

Founded in 2004 and headquartered in Newport Beach, California, GTB Technologies' enterprise DLP suite supports network DLP, endpoint DLP and discovery DLP, as well as integrated enterprise digital rights management (EDRM).

The GTB DLP product line includes the GTB Central Console server (physical or virtual instance), a single GTB Inspector installation (either physical or virtual instance) for network DLP monitoring and enforcement, the GTB Discovery server can automatically classify and scan file shares, Microsoft Exchange, any database, SharePoint and cloud storage, including Box, Dropbox, Google Drive, Azure, Office 365 and OneDrive for Business. GTB Advanced Endpoint Protector software is available for Windows and Mac OS X endpoints, servers and VDI environments, offering on- and off-network TCP scanning utilizing sensitive data fingerprints, local data discovery, complete device controls and application control with white and blacklisting, including DLP for printers.

GTB 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 inside of a virtual machine (VM) instance.

GTB is a suitable choice for organizations that need fast time to value from their DLP investment, and want a system they can deploy quickly to get actionable results.

**STRENGTHS**

GTB's combination of data fingerprinting, OCR and native SSL decryption provides powerful interception capabilities, particularly for intellectual property protection use cases.

Customers speak highly of GTB Discovery, which allows for large amounts of data to be analyzed and classified quickly from a variety of data repositories, including on-premises and cloud data storage platforms.

GTB offers its suite as a managed service; however, due to its ease of use and management, customers generally feel they do not need to continue beyond three to six months. Therefore, GTB offers this as a month-to-month-only option, without locking customers into a term commitment.

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 through native API-based integrations.

**CAUTIONS**

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 Linux.

Customers have noted that the UI could be more streamlined and more intuitive.

## InfoWatch

InfoWatch, based in Moscow, is part of a group of companies founded as an initial project by Kaspersky Lab. It has a strong market presence in Russia/Commonwealth of Independent States (CIS), as well as the Asia/Pacific region 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. The vendor provides the evidence basis for legal hold and incident investigations, as well as robust language support for DLP policy.

The primary use case for clients buying InfoWatch is control of information flows within the company and monitoring situations where employees need to have their interactions with data recorded, which are above and beyond most mainstream use cases for enterprise DLP. Gartner has observed client inquiries from countries outside of the vendor's installed base of Russia, specifically 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 2017.

InfoWatch is a suitable choice for clients that need strong network DLP capabilities, strong network-based employee monitoring capabilities for social media, text and voice, and those that require a broad range of language support.

**STRENGTHS**

InfoWatch's philosophy is largely centered on helping businesses identify disloyal employees and fraudulent activities through behavior analytics from its Traffic Monitor linguistic capabilities.

InfoWatch's linguistic analysis capabilities cover a broad range of languages, including those that are not typically supported in this market, like Hindi.

InfoWatch receives positive feedback from clients for customer experience, specifically with the ability to quickly get support engaged on incidents, and the ability to provide remote assistance.

InfoWatch supports inspection of mobile text messages, communications via mobile messengers and Skype voice calls with endpoint DLP agents.

**CAUTIONS**

Native, API-based cloud support is absent. InfoWatch does not offer discovery of sensitive data at rest in the cloud within hosted email providers or cloud storage products.

Source code detection is not a default policy, and requires additional customization of the linguistics categories in order to find source code adequately.

InfoWatch does not currently have support for Mac OS X.

Encryption or rights management based on content matching are not available remediation options within the DLP policy.

## Intel Security

Intel Security finds itself in a state of change, with the announcement of Intel selling a 51% stake in Intel Security to TPG in September 2016, with the divestiture scheduled to be completed by mid-2017.

Over the past several years, Intel Security shifted investments to and from various product lines several times without explaining these changes sufficiently within and outside the company. This has caused employee attrition at alarming rates, many of whom have either started up new security companies or are employed by competitive security vendors. There has been a chronic underinvestment in many of the Intel Security product lines historically.

The Intel Security approach has been to integrate 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 10.0 release brought further endpoint DLP enhancements and updates to the network DLP products in 2016 highlight a renewed focus from McAfee on data protection.

Intel Security is a suitable choice for organizations that have considerable resources invested in McAfee ePO and want a unified vendor that can provide DLP, device control and encryption capabilities.

**STRENGTHS**

DLP integration within the 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.

McAfee DLP includes a basic level of data classification in the DLP 10 endpoint for Windows and Mac OS X, and still tightly integrates with Titus and Boldon James for a variety of data classification options.

DLP endpoint rules are location-aware, and can have different reactions and remediations for content detection on-network versus off-network.

The Security Innovation Alliance (SIA) continues to be robust, and a good way for Intel Security customers to maximize their DLP investment due to proven and tested product integrations from data classification, digital rights management (DRM) and UEBA vendors.

**CAUTIONS**

McAfee DLP supports a native API-based integration with Box for cloud data discovery; however, other cloud applications and cloud storage support are absent.

Intel Security made some improvements to the DLP 10 agent on Mac OS X, but support for email, web and cloud are still lacking. Linux is not supported.

Clients report that DLP policy configuration can be complex and unwieldy compared to other enterprise DLP products.

Intel Security's future success in the DLP market will depend on its execution operating as its own company, and whether or not the focus can remain on the data security business for a sustained period of time.

## SearchInform

SearchInform is a new entrant to the enterprise DLP Magic Quadrant this year; it was originally founded in 1995 and is based in Moscow. SearchInform has origins in enterprise search, storage and processing of data, and in 2004 it began offering its SearchInform DLP product line to protect data. SearchInform has a strong presence in the Russian market, and also has offices in Kazakhstan, Belarus, the Ukraine and Poland. SearchInform may struggle to expand beyond its home region due to lack of adequate sales, marketing and channel resources outside of Russia. The vendor needs to expand its ecosystem if it wants to compete beyond a regional scale.

SearchInform is a suitable choice for organizations that want to take a modular approach to DLP, where some systems only enforce printing control and other systems might enforce a full suite of DLP capabilities.

**STRENGTHS**

SearchInform has strong DLP analytical capabilities, including speech-to-text transcription capabilities; however, speech-to-text is limited to the Russian language currently.

DLP endpoint agents have a modular structure, meaning that you can choose to deploy only certain capabilities, such as device control, printer control and DLP web components.

SearchInform has strong image analysis capabilities, using both OCR and its own image analysis technology.

SearchInform has strong reporting capabilities, and includes user relationship reports and cloud service usage reports among a large library of built-in reports.

Both the SearchInform AlertCenter for DLP system management and IncidentCenter for managing DLP investigations are well-designed and have simple-to-follow DLP workflows.

**CAUTIONS**

SearchInform DLP endpoint supports all major versions of Windows and Ubuntu Linux, but lacks support for Mac OS X.

Source code detection requires custom dictionaries, with no prebuilt policies for development languages.

CloudSniffer only supports Box, Dropbox, Google Drive and Yandex.

Customers cite lack of broader email visibility beyond Microsoft and the fact that the vendor does not currently support the capture of S/MIME encrypted email.

### Somansa

Somansa was founded in 1997 and first released its network data loss detection (DLD) products in 1999. The vendor has a strong Asia/Pacific region presence, and considerable operations located in its main headquarters of Seoul, South Korea. Somansa has all three major components of an enterprise DLP system — Privacy-i for endpoint DLP and discovery DLP; and Mail-i for network DLP supporting email, HTTP/HTTPS, IM and FTP protocols. Both of these products had updates in 2016.

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

Somansa is a suitable choice for organizations that need to discover data in a wide variety of repositories, including databases, CRM and ERP applications.

**STRENGTHS**

Somansa supports discovering sensitive data stored in Amazon S3, Box, Dropbox, OneDrive, Office 365, Salesforce and Google Drive using native APIs.

Customers have very positive feedback about Somansa support and its 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.

The vendor has support for discovery DLP within CRM and ERP applications, and supports a wide range of platforms and data types, including support for Informix, Microsoft SQL, MySQL, PostgreSQL and Sybase.

Somansa has endpoint DLP support for Windows, Mac OS X and Android, and is the only vendor evaluated in this Magic Quadrant that supports a local DLP discovery agent running on HP-UX and AIX.

**CAUTIONS**

Somansa does not support detection capabilities for partial document matching or unstructured data fingerprinting.

Its geographic reach predominantly consists of South Korea, with some deployments in Brazil, China, Japan, Mexico and the U.S.

Data classification is done internally to the Somansa DLP product, with no support for third-party data classification from Boldon James, Microsoft or Titus.

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 DLP market since its acquisition of Vontu in 2007. Symantec recently released Symantec Data Loss Prevention 14.5, and has product components for DLP Enforce Platform, DLP IT Analytics, Cloud Storage (supporting over 65 cloud applications), Cloud Prevent for Microsoft Office 365, DLP for Endpoint, DLP for Mobile, DLP for Network and DLP for Storage, as well as DLP API support for third-party security technologies, such as content extraction, reporting and FlexResponse for encrypting content or applying DRM. Symantec continues to invest in and improve the DLP technology in its Information Protection business unit.

In 2016, Symantec acquired Blue Coat which gives it CASB capabilities from Blue Coat's acquisition of Elastica and Perspecsys, for which there are DLP policy integrations via a bidirectional REST API between Elastica and Symantec DLP.

Symantec is a suitable choice for organizations that require advanced detection techniques and integration with CASB for data security policy uniformity.

**STRENGTHS**

Symantec offers the most comprehensive sensitive data detection techniques in the market, with advanced functionality such as form detection, image analysis and handwriting recognition 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 AWS, Azure or Rackspace connect to an on-premises DLP Enforce platform.

Symantec's SmartResponse system offers a wide range of administrative flexibility based upon content actions matching a DLP policy.

Its DLP Vector Machine Learning (VML) allows customers to train the DLP system by providing both positive and negative content examples. This could be valuable when traditional pattern matching methods are not sufficient to accurately match content.

**CAUTIONS**

Symantec clients have expressed frustration when trying to buy or renew the Data Insight add-on for Symantec DLP, which is now owned by Veritas. Ensure that your Symantec DLP reseller can also resell Veritas Data Insight if you are interested in this add-on.

Monitoring and discovery of sensitive data in cloud applications requires both DLP endpoint discovery and the required Symantec CASB Connectors in order to achieve full functionality.

Clients express concern with the overall deployment cost of Symantec DLP, when compared with competing products.

## 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, Zecurion does have a presence in the U.S., with an office in New York City.

Similar to other regionally focused vendors, the vast majority of the vendor's revenue is from operations in Russia. However, references for this Magic Quadrant included Zecurion customers outside of Russia, including U.S. customers.

Zecurion is a suitable choice for organizations that need advanced endpoint functionality, employee monitoring capabilities and tracking of DLP events over social media channels.

**STRENGTHS**

Zecurion provides full archiving of all data seen by the endpoint agent, and can also capture screen shots and other end-user screen activities.

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.

Zgate supports voice interception and file transfer captures over Skype.

The Zecurion management console supports either Microsoft SQL or Oracle database back end for event logging.

**CAUTIONS**

Zecurion does not support cloud deployment options for its management console.

The Zlock endpoint DLP agent has limited DLP capabilities for Mac OS X and Linux.

Native cloud support is lacking. Zecurion does not offer discovery of sensitive data in the cloud within hosted email providers.

Zecurion lacks support for third-party data classification, encryption or DRM products as remediation 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

CoSoSys and SearchInform are new to this Magic Quadrant.

#### Dropped

No vendors have been dropped from this Magic Quadrant.

## Inclusion and Exclusion Criteria

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

To qualify for inclusion, vendors need to meet the following inclusion criteria:

- $12 million in annual revenue specifically for their enterprise DLP products
- 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)
- Products that can solve for all three scenarios of network, endpoint and data discovery will be viewed as more complete
- 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 31 October 2016

The exclusion criteria include the following:

- Products that depend on integration into another product, including but not limited to, an email server, secure email gateway (SEG) or secure web gateway (SWG)
- Products that do not have a single centralized management interface and event workflow repository for discovery, endpoint and network DLP
- Products that use only simple data detection mechanisms (for example, supporting only keyword matching, lexicons or simple regular expressions)
- Products with network-based functions that support fewer than four protocols (for example, only SMTP email, FTP and HTTP)
- Products that primarily support DLP policy enforcement via content tags assigned to objects
- Products 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

Vendors with minimal or negligible apparent market share among Gartner clients, or with no current generally available services, may be excluded from the ratings.

Vendors that do not meet the criteria above may be included if Gartner analysts consider that aspects of the company's product, execution or vision are particularly noteworthy.

## 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 products 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 criteria 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 a new criterion to this Magic Quadrant and measures how vendors are marketing their products 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** | |
|---|---|
| **Product or Service** | |
| Weighting | High |
| **Overall Viability** | |
| Weighting | High |
| **Sales Execution/Pricing** | |
| Weighting | High |
| **Market Responsiveness/Record** | |

| | |
|---|---|
| Weighting | Medium |
| **Marketing Execution** | |
| Weighting | Low |
| **Customer Experience** | |
| Weighting | High |
| **Operations** | |
| Weighting | High |

*Source: Gartner (February 2017)*

**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, 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 DLP Magic Quadrant.

**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** | |
|---|---|
| **Market Understanding** | |
| Weighting | Medium |
| **Marketing Strategy** | |
| Weighting | Medium |
| **Sales Strategy** | |
| Weighting | Medium |
| **Offering (Product) Strategy** | |
| Weighting | High |
| **Business Model** | |
| Weighting | Low |
| **Vertical/Industry Strategy** | |
| Weighting | Medium |

| | |
|---|---|
| **Innovation** | |
| Weighting | High |
| **Geographic Strategy** | |
| Weighting | Medium |

*Source: Gartner (February 2017)*

**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 competitive visibility and execution success in specific industry sectors that are better-developed 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. There are currently no challengers in the current DLP Magic Quadrant, and there are a number of factors as to why. Niche vendors in the DLP market generally have not yet established strong global sales channels in order to achieve notable revenue, nor do they offer a complete product suite that is competitive on a broad scale with Visionaries or Leaders.

## 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, 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 form 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 evaluated for this Magic Quadrant, may be appropriate for your organization's data security needs and budget. Every organization should consider DLP through both integrated and enterprise products as part of its information security management program.

DLP technologies can be found in a wide variety of security products, as noted in "How to Choose Between Enterprise DLP and Integrated DLP Approaches." As the DLP market matures toward the Plateau of Productivity, it is becoming more challenging to develop a coherent strategy, and there is a danger of adopting an ad hoc, siloed implementation that will be difficult to monitor, manage and maintain.

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

As noted in "Hype Cycle for Data Security, 2016," DLP has continued to climb the Slope of Enlightenment toward mainstream acceptance and wide adoption. We estimate the total DLP market in 2016 to be approximately $894 million and growing at a 9.8% CAGR, to reach $1.3 billion in 2020 (see "Forecast: Information Security, Worldwide, 2014-2020, 4Q16 Update" ).

The interest in DLP did not wane in 2016. The drivers for DLP investments continue to revolve around ensuring regulatory compliance, protecting intellectual property or gaining additional visibility into data movement. While interest has remained in DLP as a technology, there are an increasing number of ways to obtain DLP capabilities, and not every organization needs to deploy an Enterprise DLP system to gain value such as through native Microsoft office capabilities, through an SEG or SWG, or by implementing UEBA to detect anomalies in user behaviors.

Over the next few years, DLP will evolve to form a core set of capabilities that will be available within specific cloud infrastructures and applications, and even embedded into client operating systems. We are already seeing this with Microsoft's approach to securing information within Office 365 and Azure Information Protection. The next major issues will be regarding how to have some semblance of data security policy uniformity across all these different operating environments and applications, and how to apply the same DLP policy on endpoints and mobile devices, and across different cloud applications. CASBs have been a promising first step, but further evolution is required to cover the wide variety of data types, data repositories and emerging applications in use by organizations.

Ultimately, DLP is faced with the inconvenient and unavoidable truth that it is not the answer for every conceivable means of data loss or theft. At present, even with extensive DLP coverage across endpoints, networks and data repositories, there are still gaps and data flows where data can leak.

The better answer is a data security strategy focused on securing the data itself, as opposed to trying to secure every system that comes in contact with sensitive data. Organizations must rethink of DLP as a "data life cycle posture," focus on unprotected and unencrypted data, and explain why data protections are not in place for sensitive data types. Information-centric security should be the rule, not the exception.

**Data Loss Prevention Is Rapidly Becoming Cloud-Centric**

Cloud usage across the enterprise has dramatically changed the expected data flows of many enterprises. With the adoption of SaaS applications and concurrently more mobile device usage and infrastructure as a service (IaaS), users might never traverse an internal network gateway before reaching these computing and storage resources, or even sending or receiving data in an unencrypted way. These changes affect how we should view traditional "data in motion," and the reality is that with cloud-hosted data, the data is constantly in motion and the data flows can be harder to predict and conceptualize. 30% of Gartner client inquiries for DLP in 2016 specifically asked for how to handle cloud data security and how to bridge the gap between DLP and protecting data in cloud architectures.

Many organizations use the integrated DLP capabilities of SEGs, SWGs and CASBs. Typically, administrators will use the built-in DLP capabilities as a first pass, and send off any more stringent policy requirements to a network DLP system before allowing data to leave the organization. This is typically accomplished through ICAP integration between a web proxy and a network DLP system. While ICAP integration remains a common requirement on RFPs, the reality is that ICAP can be an inefficient means to inspect web traffic for DLP policy. Inefficiencies exist when you force user traffic back through a corporate location before going to a remote destination. Another inefficiency could be inspecting traffic multiple times, creating unnecessary network redundancies and introducing latency. The better answer for solving data-in-motion will involve API integration between all of the different avenues for data flow (cloud applications, IaaS platforms, web traffic, etc.), and will have policy uniformity regardless of the chosen data flow. Data security policy uniformity is a key tenet of data security governance and helps to ensure that uniform controls exist across data flows, regardless of data transport.

**Microsoft's Continued Impact on the DLP Market**

While Microsoft does not meet the exact market requirements for enterprise DLP, its influence on the DLP market is undeniable. As noted in the previous version of the enterprise DLP Magic Quadrant, Microsoft has made key acquisitions in data security markets, including Adallom (a CASB), which has been launched as Microsoft Cloud App Security, and Secure Islands, which has now become the data classification foundation for Azure Information Protection Premium P2.

One common question that Gartner clients have been asking is, "Can the DLP included as part of Microsoft Office 365 and other areas of the Microsoft ecosystem replace third-party DLP systems?" One out of every eight DLP calls in 2016 related to using Microsoft's built-in DLP. Microsoft would certainly like to convince you the answer is "Yes." The short answer is simply "It depends on the organization's DLP requirements."

A number of decisions should factor into an organization deciding on whether to utilize the DLP included within the Microsoft ecosystem and some of the recent acquisitions. Some of the questions you should ask yourself, and data owners in the organization, include:

- Do we require intellectual property protection for non-Microsoft Office file types on non-Windows operating systems, where a true endpoint DLP agent is appropriate?
- Do we need to do DLP content detection using advanced techniques such as image analysis, full document matching or machine learning?
- Do we need policy uniformity between multiple applications or environments, such as the same DLP policy for Office 365, Exchange email, Slack, Salesforce and custom applications?
- Do we need sophisticated DLP discovery for multiple data repositories including unstructured and structured data?
- Do we have the appropriate Microsoft licensing in place to take advantage of these data security capabilities? Do we need to buy Microsoft Enterprise Mobility + Security (EMS) E3 or E5 bundles?

While Office 365 adoption has broached the question of using the built-in Microsoft DLP capabilities, most organizations will find that third-party data security providers are currently far more robust, including having larger predefined DLP policy libraries, and more sophisticated detection methods. As much as Microsoft would like for everyone in enterprise IT to simply apply Microsoft RMS to every file type and buy EMS E3 or E5 licenses, this is simply not an organizational or operational reality at present. Not every device operating system or file type in use is from Microsoft.

**DLP as a Managed Service Option**

Managed security services is a growing business and sized at $8.7 billion in 2015. Providers in the DLP space are offering their products as either hosted or managed services, or in "as a service" delivery models. Some of the technology providers provide their capabilities in the cloud with full management of the product, which ultimately saves the customer operational and capital expenditure costs. Examples of these vendors are Digital Guardian, Fidelis Cybersecurity and GTB. Other options involve engaging partners or global managed security service providers (MSSPs) to deliver their services as part of the partner's cloud environment; however, many of the vendors that are strong traditional MSSPs have very limited expertise managing enterprise DLP systems. Oftentimes, these larger MSSPs will partner with or contract DLP-specific expertise with either initial implementation or ongoing operational service of a DLP system.

Changes in the market for managed security services include acquisitions by vendors such as InteliSecure, a DLP-focused MSSP, acquiring Pentura, a U.K.-based managed service provider. Although Pentura was a smaller regional player, this provides InteliSecure with a broader global footprint and a platform to grow into EMEA.

Other market segments that are poised for growth include consulting for DLP. Gartner estimates the market for consulting at $17.8 billion, and it is expected to grow at an 8.5% CAGR, reaching $24.7 billion by 2020. For example, Trum Partners which is largely made up of former Vontu and Symantec employees, has a boutique consultancy with a focus on DLP, mainly Symantec DLP. Espo Systems offers similar consulting services primarily for Forcepoint product implementations. Other consultancies, such as Schedule1, are focused on providing insight into the actual risk value that can give chief information security officers (CISOs) and data owners tangible information (in dollar value) to present and get buy-in from other C-level decision makers.

### Regulatory Compliance Remains as a Main Driver for DLP Deployments

Regulatory compliance isn't going away; in fact, it is becoming more important, particularly with concerns around privacy, where DLP tools are poised to play a significant role. New regulations such as the European General Data Protection Regulation (EU GDPR) will have a global impact as of 2018, when it officially goes into effect. Also, directives such as Privacy Shield in the U.S. dictate how personal data is handled when being transferred between the U.S. and the EU, as well as non-EU countries; therefore, organizations must either augment their existing enterprise DLP tools with capabilities such as data masking and data classification, or seek new implementations to ensure compliance with new regulations.

Regulatory compliance is one of the top drivers for data security spending, especially within healthcare, banking/finance and businesses that take in a large amount of payment card data and deal with PCI DSS. Many providers of enterprise DLP tools are working hard to follow and understand the applicable regulatory requirements at the vertical level, and are orienting their products in accordance with these regulations by adding new or tweaking existing templates. This will provide end users with easy-to-implement compliance capabilities and faster time to meet the terms of the regulations.

### Intellectual Property Protection Creates a Rise in Endpoint DLP Capabilities

Intellectual property protection has been gaining interest and is identified as one of the three main use cases for enterprise DLP implementation. While most verticals have pockets of intellectual property, the main industries where it is a primary consideration include manufacturing and natural resources, financial and securities, automotive, transportation, and government, where Gartner predicts that the number of endpoints in these verticals will grow at roughly a 28% CAGR from 2017 to 2020. Other subsectors with interest in protecting intellectual property include those in the pharmaceutical and utilities markets, where they also utilize computer-assisted design (CAD) and computer-assisted manufacturing (CAM), or have patents, copyrights and trademarks. All of these sectors are expected to represent over 50% of the endpoint market in 2017. With this in mind, capabilities such as data discovery, monitoring of endpoints and applying classifications to documents with sensitive information will become important for organizations to adopt. However, endpoint DLP remains fragile, application conflicts are not uncommon and issues do crop up across all DLP vendors, even the leaders.

### Data Loss Prevention and UEBA

The insider threat is the single most difficult to control due to both accidental data loss and intentional data theft. People-centric security is a term Gartner utilizes and defines as a strategic approach to information security that emphasizes individual accountability and trust, de-emphasizing restrictive, preventative security controls and providing more visibility into an organization's overall behavior, as well as the behavior of individuals. Technology providers such as Dtex Systems, Forcepoint (with its SureView Insider Threat product) and Veriato have UEBA capabilities as part of their endpoint product strategy. Some UEBA products, such as RedOwl, include content inspection capabilities, while others specifically are not content-aware. Other UEBA vendors, such as Exabeam, Fortscale, Gurucul, Niara and Securonix, work in a complementary way with log data generated from enterprise DLP systems. Organizations can use DLP and UEBA together to implement a "trust but verify" approach whereby user activities are monitored and analyzed for misuse or malicious behavior. While it is recognized that risk will still exist, UEBA combined with DLP tools can help reduce risk significantly.

**Decisions Are Driven by a Variety of Factors as DLP Capabilities Expand**

We note that DLP capabilities are integrated into a variety of security point products, such as SEGs, SWGs, and SIEM systems, so we will see a rise in adoption of integrated DLP tools in the coming years. However, in some cases, the enterprise DLP vendors with existing deployments of SEGs and SWGs will likely win some new DLP business from vendor loyalty due to the strong argument around ease of integration. For example, in reference customer discussions, many chose their DLP provider based on existing investments of elements where DLP integrates.

Security and risk management leaders still 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. There are many use cases where integrated DLP will likely be a better fit. For example, 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. The bottom line is that organizations should not limit their view of valid DLP products 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. For more information, see "How to Choose Between Enterprise DLP and Integrated DLP Approaches."

## Evidence

Gartner used the following input to develop this Magic Quadrant:

- Results, observations and selections of enterprise DLP, as reported via multiple analyst inquiries with Gartner clients
- A formal survey of DLP vendors
- Formal surveys of end-user customer references
- Phone interviews of end-user customer references
- Gartner enterprise DLP market research data

Clearswift acquired by RUAG: "Swiss Defence Firm Snaps up Brit Security Outfit Clearswift." The Register U.K. 20 December 2016.

Forcepoint announces intent to acquire Skyfence CASB from Imperva: "Imperva to Sell Skyfence Product Line to Forcepoint for Approximately $40 million." Reuters. 8 February 2017.

Press release: Intel and TPG to Collaborate to Establish McAfee as Leading Independent Cybersecurity Company Valued at $4.2 Billion (https://newsroom.intel.com/news-releases/intel-security-tpg-partnership-mcafee/) .

Intel Security divests its firewall products: S. Kuranda. "Intel Security to Sell McAfee NGFW, Firewall Enterprise Businesses to Raytheon." CRN. 27 October 2015.

## 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.