

Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, 2Q07

Gartner RAS Core Research Note G00147610, Paul E. Proctor, Rich Mogull, Eric Ouellet, 13 April 2007, R2269 04192008

The market for content monitoring and filtering and data loss prevention technologies is maturing rapidly but remains fundamentally adolescent. The successful vendors will be those that recognize that addressing business requirements is key.

WHAT YOU NEED TO KNOW

The content monitoring and filtering/data loss (or leak) prevention (CMF/DLP) market continues to progress along the lines Gartner identified in “Magic Quadrant for Content Monitoring and Filtering, 2006.” Most market activity in the past year has centered on multichannel network monitoring, but Gartner views integrated network and endpoint control as the ultimate goal – and the ultimate destination – of the market. We have expanded our terminology to include DLP to acknowledge the different terms with which our clients refer to technologies used to prevent inadvertent or accidental loss or exposure of sensitive enterprise information. Enterprises should use CMF/DLP technologies to develop and enforce better business practices in the handling and transmission of sensitive data, and vendors should recognize that this is where their products’ true value lies. CMF/DLP is essentially risk management and security policy applied to sensitive data – finding data, wherever it resides on enterprise networks, and controlling its use, within the enterprise and beyond the enterprise boundary. Currently, CMF/DLP tools are extremely helpful in reducing accidental data leakage and are somewhat helpful in reducing deliberate attempts to circumvent corporate data dissemination policies. CMF/DLP tools classify data “on the fly,” which is useful because most organizations have failed to produce policies and processes such that users can be trusted to do it themselves. CMF tools classify data dynamically, and then dynamically apply the desired type and level of control, including the ability to perform mandatory access control (cannot be circumvented by user). The nine vendors that met Gartner’s strict definition of this market and the vendors listed in Note 1 provide many good choices for organizations seeking content-aware DLP capabilities.

MAGIC QUADRANT Market Overview

The CMF/DLP market (which Gartner has identified in previous Magic Quadrants as the CMF market) includes vendors of technologies for defining sensitive information, finding and identifying it on enterprise networks and in storage, and controlling its use and distribution. These technologies are emerging as important information security controls. One of the key drivers of this market is the need to address regulatory requirements, including those of the Payment Card Industry (PCI) Initiative and the U.S. Health Insurance Portability and Accountability Act (HIPAA).

This market is a small one – defined by Gartner as being in its “adolescent” phase – but it is experiencing rapid growth. The market’s total value for 2006 was an estimated \$50 million, and Gartner predicts that it will reach \$120 million to \$150 million in 2007. Customers should expect significant market turmoil through 2008, with some vendors going out of business, merging with others or being acquired by major security vendors. A key driver in the market’s ongoing maturation was the infusion in 2006 of significant amounts of venture capital into relatively small vendors, with many vendors receiving funding in the \$30 million to \$40 million range. The result has been that these better-funded vendors have acquired more capable and experienced management, and the quality and capabilities of their products have generally improved in the past year.

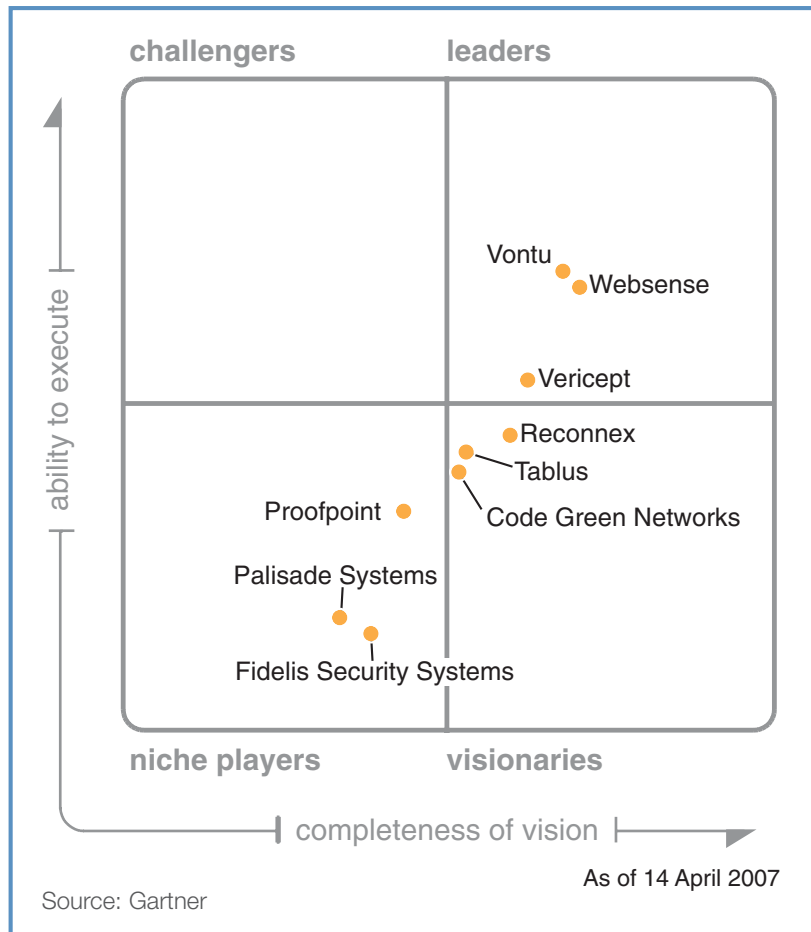
The content awareness mechanisms that are central to CMF/DLP technologies can also be found in other products – for example, e-mail security, instant messaging (IM) and endpoint monitoring solutions. Nonetheless, a stand-alone (or “pure play”) CMF/DLP tool, anchored by strong, content-aware network monitoring capabilities, remains the best solution to the problem of identifying and controlling sensitive enterprise data, because it can monitor multiple channels for specific inbound and outbound content. Gartner continues to exclude exclusively host-based (endpoint) solutions from the Magic Quadrant because of market readiness and technical challenges. Our clients continue to express concerns that agent-based solutions are more difficult to manage, have more-primitive detection techniques and fail to protect unmanaged systems. We maintain that at this stage of market development, it is unreasonable to expect enterprises to deploy an agent on every desktop to enable agent-based capabilities. Network capabilities alone have significant limitations as well, such as the inability to detect or prevent any sensitive data operations that do not pass through one of the CMF/DLP network sensors. For this reason, endpoint capabilities will eventually be critical, but Gartner believes that endpoint agents will never eliminate the need for network monitoring, and so a combination of both approaches is ideal. Current endpoint tools tend to have much more limited capabilities and – though they are rated higher than in 2006 – endpoint capabilities are still weighted relatively low in this Magic Quadrant.

The CMF/DLP market continues to follow the evolution that Gartner predicted in the 2006 Magic Quadrant, which has four basic phases:

The Magic Quadrant is copyrighted April 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner’s analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2007 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner’s research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

Figure 1. Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, 2Q07



- Phase 1: E-Mail Only – Monitoring e-mail using basic key matching or regular expressions. Gartner excludes these technologies from the Magic Quadrant because of our requirement for multichannel monitoring.
- Phase 2: Data in Motion (Network) – Monitoring multiple network channels (typically IM, FTP, HTTP and generic TCP/IP) using more-advanced detection techniques. This area of the market has matured in the past year.
- Phase 3: Data at Rest (Discovery) – Analysis of static, stored data to identify sensitive data, wherever it may be stored in the enterprise. This includes integration with document management systems and basic endpoint agents without true content-analysis capabilities.

Note 1 Alternative Solution Vendors

The CMF/DLP market is adolescent and growing. For this reason, a number of vendors have positioned themselves in this market, but they do not meet Gartner's relatively conservative definition. These include endpoint-centric vendors, and those that are too small or do not have sophisticated detection mechanisms. This market is evolving, and Gartner's market definition will evolve with it. The following alternative solution vendors may be of interest, depending on your requirements.

Workshare

Workshare started by offering a metadata cleansing product, primarily used in verticals (such as the legal industry) with high degrees of concern about inappropriate content leaving the organization in documents. The Workshare product, deployed on the endpoint, has since added basic CMF/DLP capabilities, using contextual analysis, keywords and regular expressions. In 2006, Workshare added network-based e-mail and Web filtering using the same policies, and the company sells a separate product for content discovery. Workshare was not included in the 2007 Magic Quadrant because of the limited channels covered by the network product, its lack of advanced content analysis and the insufficient enterprise installed base and references for the newer network product. Workshare is not considered a competitive CMF/DLP product at this time, but the company's strategy indicates plans to move more strongly into this market.

Oakley Networks

Oakley Networks provides limited content awareness in a predominantly endpoint solution with some network-based components. The solution is best employed as an endpoint monitoring and targeted investigation tool.

GTB

GTB Technologies is a new entrant in the CMF/DLP market and did not meet the inclusion criteria because of lack of available references and a small installed base.

Orchestria

Orchestria began as a CMF solution developed specifically for the financial services market, with an emphasis on monitoring and enforcing broker/trader compliance primarily through conceptual analysis with a combined endpoint/network solution. The company was not included in this Magic Quadrant because of network monitoring limitations and the requirement for an endpoint agent for full functionality. Orchestria is beginning to move into the generic CMF market and should be watched closely as it releases broader-based solutions.

Secure Computing

With the 2006 acquisition of CipherTrust, Secure Computing gained individual products for e-mail, Web and IM monitoring and filtering. These products are primarily focused on inbound threat mitigation, but each includes basic CMF capabilities. Secure Computing was not included in the Magic Quadrant because of lack of an integrated management and policy interface dedicated to CMF across its product lines.

Clearswift

Clearswift has separate products for e-mail and Web filtering, both with outbound CMF capabilities. These features have been part of the Clearswift product line for several years. Clearswift was excluded because of a lack of common management and policy interface dedicated to CMF.

Verdasys

Verdasys is an endpoint-only solution vendor with some CMF capabilities, particularly auditing and blocking, but with only limited content awareness. The company recently added content analysis, through the use of the Autonomy engine. Verdasys has claimed data protection capabilities since its inception, but this is the first Verdasys product release to include content, rather than just context, and it has yet to be tested widely in the market. Verdasys will need to add or partner for network capabilities before its product can be considered a complete CMF solution.

McAfee

In 2006, McAfee acquired Onigma, a small Israeli startup with an endpoint-only CMF product. McAfee is integrating the Onigma technology into its endpoint security suite, but, as with all endpoint solutions, it will need to add network capabilities to be considered a complete CMF product.

Provilla and NextSentry

Provilla and NextSentry are endpoint CMF solution vendors facing the same challenges as McAfee and Verdasys, but they lack the larger installed base of those competitors.

Source: Gartner

- Phase 4: Endpoint – The successful blocking of all channels at the endpoint, including the network interface and within the operating system and between applications. This nascent segment of the market is very small but growing. Vendors have significant plans in this area, although real-world product offerings with competitive CMF/DLP capabilities are unlikely to become available in 2007.

Phases 1 and 2 involve devices that reside at the edge of the network, while Phase 3 includes a combination of network and host technologies. The nascent Phase 4 – which Gartner believes represents the ultimate destination of this technology and market – involves agents that reside on a local host, and it requires much-deeper integration with servers and desktops.

Market Definition/Description

Gartner defines CMF/DLP technologies as those that – as a core function – perform deep packet inspection on outbound network communications traffic, track sessions and perform linguistic analysis to detect, block or control the usage of (for example, saving, printing or forwarding) of specific content based on established rules or policies. The channels to be monitored include e-mail traffic, IM, FTP, HTTP and other TCP/IP protocols. Linguistic analysis must use techniques that extend well beyond simple keyword matching (for example, advanced regular expressions, partial document matching, Bayesian analysis and machine learning).

Many security professionals view these technologies as primarily concerned with protecting intellectual property and other valuable enterprise data from theft. Gartner maintains, however, that their true value lies in helping management to identify and correct faulty business processes and – crucially – identify and prevent accidental disclosures of sensitive data. This concern is becoming more and more important because of the compliance demands of regulatory initiatives (for example, breach disclosure laws and HIPAA) and industry initiatives, such as the PCI standard. This is why Gartner has chosen to rename this market as CMF/DLP, to reflect the growing demand for technologies that do not simply address insider theft and malicious attacks – an area in which CMF/DLP technologies have, in any case, comparatively limited capabilities – but help to identify bad practices that place sensitive data at risk and offer means of limiting such risk.

Inclusion and Exclusion Criteria

Vendors are included if their products:

- Perform content-aware deep packet inspection on outbound network communications traffic, including e-mail and other protocols
- Track complete sessions for analysis, not individual packets
- Use linguistic analysis techniques beyond simple keyword matching for detection (for example, advanced regular expressions and document fingerprinting)
- Detect (or filter) content that is based on policy-based rules
- Monitor network traffic for, at a minimum, e-mail traffic and other channels/protocols (for example, HTTP, IM or FTP) and analyze across multiple channels, in a single product and using a single management interface
- Block, at a minimum, policy violations over e-mail
- Were generally available as of 1 December 2006
- Are deployed in customer production environments, with at least three references

Participants must also be determined by Gartner to be significant players in the market, via market presence or technology innovation, or both.

Agent-based products unable to monitor traffic from unmanaged systems (those without an agent) were not considered for evaluation.

Added

Vendors added include:

- Code Green Networks
- Websense – Acquired PortAuthority Technologies

Dropped

Vendors dropped include:

- Intrusion – No longer meets Gartner's inclusion criteria
- PortAuthority Technologies – Acquired by Websense

Evaluation Criteria

Ability to Execute

Gartner weights Ability to Execute heavily toward product capabilities, because most of the vendors in this adolescent market are still comparatively new. Our ratings are most influenced by three basic categories of capability:

- Performance – The maximum bandwidth at which traffic can be effectively analyzed. Preference is given to products that can “scale” to operate in large enterprises (in the 200-Mbps to 500-Mbps range).
- Manageability and workflow – The primary value of CMF/DLP technologies lies in their ability to solve business problems, and they are typically used by technical and nontechnical staff. For this reason, Gartner gives preference to products capable of strong segregation of duties and user-friendly management interfaces, with robust and well-integrated incident handling and administration and case management capabilities.
- Core technology – Preference is given to products with the greatest product maturity and capabilities, especially in:
 - Range of channels monitored
 - Range of blocking capabilities
 - E-mail integration
 - Range of detection techniques
 - “Data at rest” content discovery capabilities

Completeness of Vision

The CMF/DLP market, while still comparatively new, is rapidly becoming mainstream, Vendors are acquiring more capable management, and vendors' products are acquiring greater breadth and depth of capabilities. However, the market remains intensely competitive, and it is likely to become even more so. For this reason, Gartner gives strong preference to vendors that demonstrate completeness of vision – in terms of strategy for the future – and ability to execute on that vision. We continue to expect more established security vendors to enter and eventually

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	standard
Market Responsiveness and Track Record	high
Marketing Execution	standard
Customer Experience	high
Operations	standard
Source: Gartner	

PortAuthority product offers advanced analysis techniques with broad channel coverage, as well as good workflow. Although Websense offers new endpoint support through an OEM deal with Safend, Gartner expects the company to integrate its existing Client Policy Manager (CPM) endpoint agent with the PortAuthority product. Websense will be challenged to avoid mandatory bundling of its CMF/DLP and URL filtering product lines, which appeal to different buying centers and could inflate prices. Vericept – which edged into the Leaders quadrant in 2007 despite some reports of incomplete features being released – improved

considerably in 2006 and appears, along with Vontu, in most major competitive evaluations. Vericept is innovating quickly but only recently properly aligned product positioning to best capitalize on the market, and it will need to improve sales channels and product maturity in 2007 to maintain its position. Vontu remains a strong option and offers some of the best overall product maturity. While Vontu innovation has slowed, the company's features are mature and well-integrated when released.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	high
Offering (Product) Strategy	high
Business Model	high
Vertical/Industry Strategy	low
Innovation	high
Geographic Strategy	low
Source: Gartner	

Vericept

Vericept offers a broad CMF/DLP product suite with network monitoring and filtering (filtering is embedded for e-mail and, through Web gateway integration, for HTTP) and data-at-rest content discovery. Near the end of 2006, Vericept introduced a desktop agent, but this was not available through all channels and lacked sufficient production deployments for full evaluation. In 2006, Vericept was striving to regain market leadership and reposition its product to better address the CMF/DLP market. Vericept improved its stability, performance and features – especially its detection techniques – but Gartner still receives reports of stability and support issues from nonpremier Vericept clients. Vericept initially started as an acceptable-use enforcement product, and it offers the broadest category set for detection of sexual harassment, gambling and other unapproved activities. Vericept's Content Analysis Description Language (CANDL) for adding detection techniques shows promise, despite some initial deployment issues. Vericept's pricing seems to vary more widely than other CMF/DLP vendors', and the company appears in many competitive evaluations.

Shortlist: Vericept should be on the shortlists for midsize to large enterprises that want a broad product suite, especially those seeking to integrate acceptable use with loss prevention.

dominate the market, so we place a stronger emphasis on products than on marketing or sales strategies. A clear understanding of the business needs of CMF/DLP customers – even those who do not fully recognize those needs themselves – is an essential component of vision. This means that vendors should focus on enterprises' business- and regulation-driven need to identify, locate and control the sensitive data stored on their networks and passing their boundaries.

Leaders

As expected, two additional vendors entered the Leaders quadrant this year, while Vontu maintained its status. Websense acquired PortAuthority in January 2007, after a short strategic partnership, combining the sales and marketing strengths of a large vendor with a smaller player's reasonably strong product capabilities. The

Vontu

Vontu offers four product lines, with network monitoring, network blocking (via integration with third-party e-mail and Web gateways), data-at-rest discovery, and data-at-rest protection (via quarantine or encryption). A desktop agent was in testing at the time of this Magic Quadrant and was not evaluated. All product lines are well-

integrated into a single management console with a single policy engine, and they support a variety of detection techniques for structured and unstructured data. Vontu has the largest installed base of large enterprises in the CMF/DLP market. Vontu initially led the CMF/DLP market in innovation, but as its customer base has increased, its rate of innovation has slowed, and other vendors are often first to market with key features. Nonetheless, features released by Vontu tend to be stable and well-integrated, whereas other vendors may rush features to market. The largest dedicated CMF/DLP vendor in terms of revenue, and appearing in nearly every major selection process, Vontu tends to be the least flexible in pricing, and some prospects have complained to Gartner about aggressive sales tactics.

Shortlist: Vontu should be on the shortlist for large enterprises and other enterprises with sufficient budgets that want a well-integrated and stable product with excellent workflow.

Websense

Websense provides fundamentally solid CMF/DLP functions for data in motion (network) and at rest (discovery) in the same appliance. The company uses advanced detection techniques, including partial document match, data fingerprinting and statistical analysis to detect character replacements. Competitive differentiators include network printing analysis and watermarking as a response, offered through a partnership with SourceMedia (formerly Thomson Media). The ability to offer end users self-remediation for quarantined e-mails, such as encrypt and forward, can reduce operation costs. The product is internationalized to be able to detect content in double-byte character sets – a capability that is already in use in Japan – but the user interface is not localized.

Websense acquired PortAuthority in January 2007 after a strategic partnership in 2006 and has announced that it intends to integrate the two companies' technologies in 2007. Before the acquisition, PortAuthority provided host functions through a partnership with Safend. The integration with Websense technology will likely involve integrating content awareness capabilities into the Websense Client Policy Manager host agent. Given the stability of its host-based technology, Websense should be well-positioned to provide a comprehensive solution for data in motion, at rest and endpoint.

Shortlist: Websense should be on the shortlist of any enterprise that requires comprehensive CMF/DLP functionality.

Challengers

There are no challengers in the 2007 CMF/DLP Magic Quadrant.

Visionaries

Three vendors – Code Green Networks, Reconnex and Tablus – are ranked as visionaries in the CMF/DLP market, but, surprisingly, none achieved a higher Visionaries rating than any of the leaders. Reconnex rose into the Visionaries quadrant because of dramatically improved product strategy, positioning and product capabilities. Instead of relying on its forensic “historical enforcement” capabilities, the company began development of a full CMF/DLP product suite. Tablus was unable to capitalize on its 2006 Visionaries rating and slipped slightly from last year, because of an overly intense focus on one large enterprise client. The plans

announced for 2007 indicate that Tablus will maintain a Visionaries position in the market, but the company could face further challenges if it does not improve its execution. Code Green Networks, a new entrant in 2007, is designated as a visionary because of its business model and tight focus on the small and midsize business (SMB) market. Product capabilities definitely lag other leaders and visionaries, but the simple packaging and management interface, combined with aggressive pricing, may prove successful in the midmarket and “buy” Code Green Networks the time to improve its comprehensiveness and attack the larger-enterprise market.

Code Green Networks

Code Green is a well-funded startup targeting the SMB market with a reasonably priced appliance. The company's Content Inspection Appliance can monitor a network channel passively or act as a message transfer agent (MTA) but provides no discovery functions. (An endpoint agent was added – through a partnership with Centennial Software – too late to be evaluated for this Magic Quadrant.) The interface is wizard-driven, with the goal of serving users outside IT organizations. The product is internationalized to handle detection of double-byte content, and the interface has been localized in English and Japanese. The primary detection mechanism is registered data partial document matching, with each appliance designed to fingerprint 1TB of data and detect the transmission of as few as 300 characters. Each appliance must be managed separately, and delegated administration is not very sophisticated. Code Green is in the Visionaries quadrant because it has the opportunity to grow beyond its SMB roots and become a leader by 2008 or 2009 – if it can execute effectively.

Shortlist: Smaller companies that focus on network DLP, with data stores of 1TB or less, should put Code Green Networks on their shortlists.

Reconnex

Reconnex offers data in motion (network) and data at rest (discovery) components in a single appliance with good delegated administration. Advanced detection techniques include partial document matching and the ability to detect modified text. One substantial differentiator is Reconnex's case management capability, which is the most sophisticated of any product in this survey, and it is tied to a good forensic capability that correlates events for investigations and can selectively record all communications traffic, not just policy violations. Historical data can help organizations with remediation and rule tuning. Reconnex moved from Niche Players status to the Visionaries quadrant this year, and it has the ability to become a leader with continued execution.

Shortlist: Reconnex should be on the shortlist for midsize to large enterprises that want broad CMF/DLP capability, especially those looking for forensic capabilities and good case management.

Tablus

Tablus has data in motion (network), endpoint, and data at rest (discovery) components. In addition to having all three primary components, the company is differentiated by its temporary agent architecture for discovery and a capture engine that “crawls” data to determine, based on sophisticated described data techniques, that which is sensitive in a large group of files. The temporary

agent architecture reduces the resources required to detect sensitive data at rest, making distributed discovery more practical than solutions based on file shares. One shortcoming is that the discovery function and network function use different interfaces and different policy definitions.

Shortlist: Tablus should be on the shortlists of organizations that are focused on data in motion and that have large file repositories and lack clarity about their sensitive data. Tablus is also a good choice to address requirements for detection of data at rest in large distributed environments.

Niche Players

Niche Players include Fidelis Security Systems, Palisade Systems and Proofpoint. Proofpoint slipped from Challengers to Niche Players status because it failed to keep pace with a rapidly changing and growing market and remained highly e-mail-centric. Proofpoint lacks full channel coverage and discovery capabilities, and its management interface still treats all policy violations as if they were e-mail violations, regardless of the channel used. Fidelis' product remains the only all-channel blocking solution on the market, but it still suffers from execution issues, and it lacks any discovery capabilities; the product's e-mail integration is poor, relying on TCP resets for blocking, although Fidelis plans to improve this in 2007. Palisade combines URL filtering, threat management and CMF/DLP into a single product. This may appeal to certain SMBs, but weak workflow and lack of discovery and other CMF/DLP features limit Palisade's penetration of large enterprises.

Fidelis Security Systems

Fidelis offers network monitoring and filtering in a dedicated appliance with integrated all-channel blocking. Fidelis supports private data protection through its Smart Identity Profiling feature, but it does not support partial document matching or other advanced unstructured data protection. All Fidelis blocking is done using TCP resets or dropping traffic when deployed as a network bridge – approaches that offer broad filtering but no user feedback and is not recommended for e-mail. Fidelis does not offer a data-at-rest content discovery product or features. Reports from independent evaluations indicate that the Fidelis product suffers from false positives and requires more tuning. Fidelis has lagged in 2006 and will continue to struggle in 2007 unless major improvements are made.

Shortlist: Organizations that need all-channel blocking in a single appliance, and do not require unstructured data protection should place Fidelis on their shortlists.

Palisade Systems

Palisade remains a small vendor in the overall CMF/DLP market, with a unique approach that combines URL filtering, intrusion detection/threat management and CMF/DLP. The company possesses the capabilities to innovate but does not seem to fully capitalize on its successes. Palisade continues to experience a lack of exposure on larger requests for information/requests for proposals (RFIs/RFPs), primarily because of limited capabilities in its CMF/DLP workflow. Client deployments seem to continue to lean heavily on Palisade's URL filtering capabilities.

Shortlist: Palisade remains attractive to small and midsize organizations that are looking for a single-vendor solution to address several requirements and have determined that they do not require complex integrated CMF/DLP workflow.

Proofpoint

Proofpoint, which is primarily a secure e-mail boundary (SEB) vendor, introduced CMF/DLP capabilities in late 2005. Proofpoint can monitor and enforce e-mail policies, with an additional monitoring appliance for HTTP and FTP traffic and IM through partnership. Proofpoint is extremely e-mail-oriented and lags behind other CMF/DLP vendors, because it has no data-at-rest discovery, limited channel monitoring and an e-mail-oriented workflow that does not translate well for other communications protocols. Proofpoint's CMF/DLP products are routinely sold to existing e-mail gateway clients, or e-mail-centric customers, and they are not typically seen in dedicated CMF/DLP evaluations.

Shortlist: Existing Proofpoint clients looking to add basic CMF/DLP capabilities and Web-only monitoring should place Proofpoint on their shortlists.

Vendor Strengths and Cautions

Code Green Networks Strengths

- Reasonably priced appliance for SMBs
- Internationalization

Cautions

- Limited value for larger enterprises
- Appliance management and delegated administration

Fidelis Security Systems Strengths

- All-channel blocking
- Dedicated appliance

Cautions

- Poor detection performance.
- Limited capabilities – Product lacks many core CMF features.
- Vendor struggling to adapt to the market and acquire positive revenue stream.

Palisade Systems Strengths

- Integrated CMF, Web filtering and threat management

Cautions

- Poor workflow.
- Limited capabilities – Product lacks many core CMF features, such as discovery.

Proofpoint

Strengths

- Combined e-mail security with inbound and outbound monitoring/filtering

Cautions

- Extremely e-mail-centric product.
- Monitors only Web/FTP and e-mail traffic (IM available through partnership; enforcement on e-mail only).
- Limited capabilities – Product lacks many core CMF features, such as discovery.

Reconnex

Strengths

- Forensics and case management
- Well-designed interface

Cautions

- Defining and tuning sensitive data are sometimes challenging.

Tablus

Strengths

- Distributed data-at-rest discovery in larger enterprises

Cautions

- Lacks consolidated interface for network, endpoint and discovery

Vericept

Strengths

- Broad platform coverage, including network monitoring/filtering, discovery and a new endpoint agent
- Extensive acceptable-use categories

Cautions

- Some features released to market before full maturity.
- Product may fail to “sampling” mode when capacity exceeded (not including e-mail when using the embedded MTA).
- Some reports of variable pricing when customers fail to negotiate strongly.

Vontu

Strengths

- High product maturity and comprehensiveness of coverage
- Strong workflow and management interface
- Proven track record in large enterprises

Cautions

- Discovery (data at rest) performance that does not scale well for very large storage repositories
- Little pricing flexibility
- Some reports of overly aggressive management tactics

Websense

Strengths

- Large, stable business; unlikely to be acquired
- Advanced detection techniques

Cautions

- Integration plans that may stall innovation through 2007

Vendors Added or Dropped

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

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

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

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

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

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

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

Completeness of Vision

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

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

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.