

Magic Quadrant for Mobile Data Protection

Gartner RAS Core Research Note G00169804, John Girard, Eric Ouellet, 1 September 2009

Mobile data protection products secure data on movable devices that can leave the office, including notebooks, PDAs and smartphones. Buyers want products that work equivalently across multiple platforms, need minimal support, provide for common policies and extend protections to removable media.

WHAT YOU NEED TO KNOW

Mobile data protection (MDP) systems and procedures are needed to protect data privacy and to comply with audit requirements, and every company must include MDP in its IT operations plan. This Magic Quadrant (see Figure 1) is a snapshot of the overall market. The Leaders quadrant denotes vendors with a balance of strengths. However, vendors in any category, as well as those not ranked on the Magic Quadrant, may be more appropriate for your enterprise's needs and budget.

MAGIC QUADRANT

Market Overview

MDP for notebooks and smaller handheld devices (PDAs and smartphones) is a growing market with two primary purposes: first and foremost, to protect data by encryption; and second, to provide evidence that the protection is working. Most vendors in this market started on desktops, but the clearly defined buying center is mobile, and the primary source of revenue comes from installation on notebook computers. The MDP market has been led for years by small independent software vendors (ISVs), some of which have been in the market for up to 25 years. However, mergers and acquisitions are handing the reins over to broader endpoint protection (EPP) vendors. Protection schemes embedded in hardware or the operating system (OS) are incomplete, and leave plenty of room for ISVs to compete for years to deliver common, cross-platform policy management.

Interest in data protection is fueled by liability and privacy concerns. Across the U.S., legislation is increasing to require public disclosure in the event of the real or suspected mishandling of personally identifiable information. Civil and criminal penalties for data leaks, and pressure to disclose leaks, are also growing in other countries. Even if information is not misused, negative public reaction is expensive and embarrassing, and it damages buyer and investor confidence.

Demand for products in this market continues to grow, although the current economic crisis has slowed the rate and size of purchases. The following information is derived from the 2009 Magic Quadrant survey results: Seats sold for 2008, and estimated for 21 vendors (15 reporting), totaled about 28 million, compared with almost 26 million estimated for 18 vendors in 2007, and 14 million seats tallied for 15 vendors in 2006. In last year's report, rapid growth in the first half of the year supported a prediction that seat sales could double for this report,

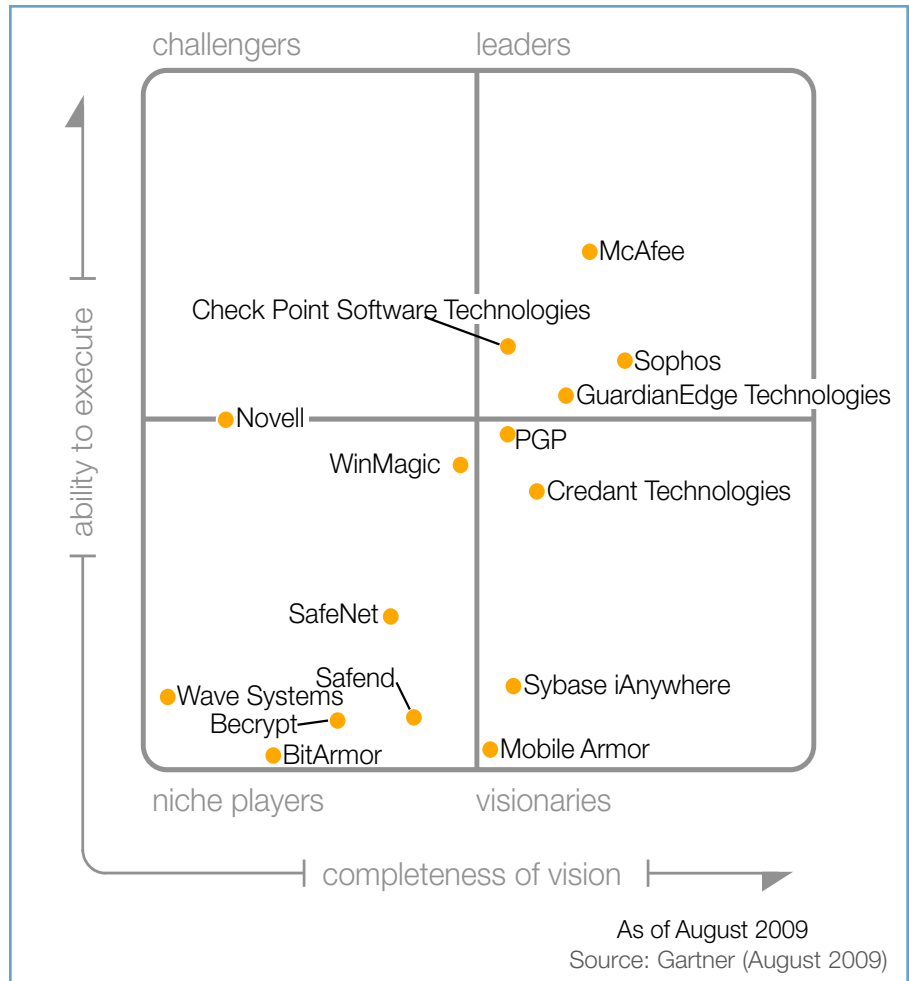
but ultimately, growth was limited. The small increase over last year's report is partly due to reduced sales owing to the economy, and partly due to revised prior estimates. Gartner believes that sales were attenuated by delays in acquiring mobile data protection products, and the diversion of funds into higher-priority projects. Average sales per vendor in 2008 were about 1.3 million seats, with a median of approximately 650,000. Three-year cumulative seats sold (2006+2007+2008) are estimated at approximately 64 million.

Revenue growth in the market is positive, with all but a few companies showing some level of increase. According to information derived from the 2009 Magic Quadrant survey results, 2008 worldwide revenue in the MDP line of business (LOB) is estimated at \$716 million, compared with \$611 million in 2007, \$432 million in 2006 and \$287 million in 2005. Performance is spread among a few large vendors and many small vendors, creating a median performance of \$17 million and an average of about \$38 million. It should be noted that LOB revenue does not map directly to MDP seat sales, since larger vendors include multiple products in the LOB that supports MDP. LOB revenue is always useful to gauge company health and ability to execute.

Software as a service (SaaS) is available through several vendors in the survey. SaaS means that the customer offloads the cost and management of the policy server, and pays a lower per-user seat charge. In general, and with few exceptions, SaaS represents a small percentage of earnings for vendors tracked in this report.

Client inquiry calls steadily continue to request assistance in understanding, choosing and implementing data encryption. The number of calls and the size of pending installations suggest that data protection is still inadequate across industries. Owing to current economic problems, many companies continue to install encryption on a subset of their workstations, which means that the opportunities to sell new licenses will exist for years into the future. Stories of stolen devices containing exposed data continue to proliferate, and have not reduced in severity from prior years. Each year, hundreds of thousands of laptops, and potentially millions of smaller devices, are estimated by various sources to

Figure 1. Magic Quadrant for Mobile Data Protection



go missing through loss or theft, or are upgraded or exchanged without first having their data removed. Others fall prey to network-borne attacks and data copying, but data protection can't protect from these types of attacks. Data loss and theft are also increasing through removable portable storage devices that impact authorized users, as well as those who lose their storage media.

Increasing legal and regulatory demands for the protection of data will maintain a hot interest in this market and topic for many years. In the U.S., for example, most states have enacted data breach disclosure laws. The number of systems that lack protection continue to outrun the sales in this market by margins that ensure continued MDP sales. For example, Gartner's 2009 forecast for

The Magic Quadrant is copyrighted August 2009 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.

© 2009 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.

new sales of mobile PCs used by professionals is expected to reach more than 148 million units, thereby contributing to an active installed base of more than 447 million. That estimate does not include home PCs used for business purposes, nor does it include millions of smartphones that need managed protection. To date, many companies have only made small investments in MDP products, and the three-year cumulative seat sales estimated at 64 million are only a good start in solving data protection problems.

Continuing innovations within the market, growth in products' scopes to encompass more related functions in the areas of EPP, content monitoring and filtering (CMF), and data loss prevention (DLP), generally positive (although attenuated) overall financial performance, and continuing strong client interest have earned the MDP market a promising growth potential rating in 2009. Buyers should continue to make incremental investments, and must be prepared to reassess vendors on an annual basis, taking into account future consolidations and exits of point solution vendors, as well as disruptive emerging technologies, such as hardware encryption.

Several promising vendors in this market are small enough in terms of revenue to represent acquisition targets, and Gartner continues to see interest from investors and larger security vendors.

Client Concerns for 2009 and 2010

Gartner clients know that data leakage can cost them money and reputation, and eventually most companies will make MDP investments, whether they are small or large enterprises, or bound by compliance rules or not. They will make those purchases faster when the solutions are easy to understand and manage, easy to use, and priced affordably. With potentially dozens of products to choose from in the MDP market, and many more in tangential encryption markets, the majority of prospective buyers are following two paths. Companies that are most constrained in the current economic climate will make minimal investments on the assumption that only a few systems are at risk, and they will likely purchase point products from several vendors rather than a comprehensive solution. Companies that understand that data encryption administration can be passed to the operations team along with antivirus (AV) are more likely to look for package deals from their EPP providers.

Buyers that have struggled with point solutions will give weight to vendors that can support platforms, large and small, with a similar look and feel, as well as provide common security and auditing policies. In 2009, the fruits of mergers between MDP vendors and EPP vendors have raised the value proposition from simple coexistence, and have begun to deliver tangible alignment among configuration management, encryption, host intrusion prevention systems (IPSs), personal firewalls and anti-malware defenses. Of particular visibility in this regard are Sybase iAnywhere, Check Point Software Technologies (acquired Pointsec Mobile Technologies), McAfee (acquired SafeBoot), Sophos (acquired Utimaco Safeware) and Symantec (pursuing a close partnership with GuardianEdge Technologies). Other opportunities arise when vendors pursue partnerships for software distribution, asset tracking, backup/restore, inventory and other nonsecurity operations. These partnerships make it easier for enterprises to prove that user endpoint systems are secure and up to date, and can reduce the total cost of ownership of supporting multiple endpoint agents.

Package deal pricing from the EPP vendors is extremely attractive. EPP vendors have suffered several years of eroding prices because their AV products have been driven to commodity status. MDP products, on the other hand, have maintained high seat prices even in large quantities. EPP vendors can afford to start high and discount MDP; in the end, they earn a combined seat price that is many times higher than they could collect alone for endpoint AV, firewall and IPS. Those discounted prices ultimately constrain the point solution MDP vendors that can't afford to undercut.

Hardware subsystems, including the trusted platform module (TPM) and Seagate's encrypting hard drives, have raised client awareness and interest in the potential of hardware systems to strengthen data protection and improve performance, but they are not universal solutions for all applications and all platforms. Buyers have found it difficult, in terms of sourcing and incremental cost, to integrate these systems for large adoption across all their platforms. Beginning in 2010, the availability of hardware encryption will improve dramatically, with common use established by 2015 as a result of events started by the Trusted Computing Group (TCG). On 29 January 2009, TCG, a not-for-profit organization that develops open standards for hardware-enabled security technologies, released three final specifications for a standard for managing hardware-level data encryption. TCG reports that almost all major storage manufacturers have indicated that they intend to adopt the new standard and deliver products by year-end 2009. No hardware system is ready to be a complete solution unto itself. ISVs in the market are increasingly taking advantage of these hardware systems when they are present, but at the same time, these hardware systems can offer strong protection in software without them. For additional information, see "Trusted Computing Group Specifications Will Simplify Hard-Drive Encryption."

Microsoft's BitLocker caused a lot of anticipation among buyers and some angst among MDP vendors, but never became a market force. Weak adoption of Vista limited the percentage of systems that could benefit from it. Several ISVs have released management support for BitLocker as well as Windows Encrypting File System (EFS), so clients can find ways to use these functions when desired.

Key management, storage and destruction methods are frequently on buyers' minds because of concerns regarding recovery of lost user/system access credentials, as well as for data destruction. Well-managed key destruction is tantamount to drive wiping, and is essential to defend against data breaches on lost systems. It also provides a low-cost, low-risk, green method to dispose of old drives.

Removable media protection is a subject raised in every client inquiry. MDP vendors have responded with encryption policies and port controls based on user certificates, application type, document type and device type. Portable viewing systems for encrypted documents are also offered. Dedicated products continue to sell as point solutions and are preferred by some clients that value particular features, such as tamper-proof flash drives.

Government security certifications are generally expected by nongovernment purchasers. Enterprise buyers want to see that vendors are serious about delivering the best protection, and they recognize U.S. Federal Information Processing Standards (FIPS), Common Criteria (CC) and other designations as proof of vendor

commitment (see the “Vendor Strengths and Cautions” section of this research for lists of vendor certifications). Readers should note that vendors may accrue a long list of certifications for algorithms for encryption, key management, quality management and specific countries. This research primarily considers FIPS 140-2 because it is a rigorous and internationally recognized certification for cryptographic engines. CC certification is considered ahead of country-specific and industry-specific certifications, again, because it is, by design, internationally recognized.

In June 2007, U.S. federal Blanket Purchase Agreements were awarded, in a joint effort by the U.S. Office of Management and Budget, the U.S. Department of Defense and the U.S. General Services Administration (GSA), to several of the vendors tracked for this Magic Quadrant. These blanket purchase orders can sometimes be used by other agencies, including state and local governments, and stimulate sales opportunities by virtue of expedience. During 2008 and 2009, Gartner observed the positive effects of the GSA’s SmartBuy program in client purchase decisions. Although no additional vendor awards have been given, Sophos has cleverly arranged to sell under the award granted to the Information Security Corporation (ISC).

Market Definition/Description

Products that Gartner tracks in the MDP market are software utilities that enforce data privacy policies by managing data encryption on the primary storage system of mobile platforms, including notebooks, PDAs and phones. MDP products operate as active services bound to the OSs and basic input/output subsystem (BIOS) services of their host platforms, so that they can control primary storage I/O and assert themselves in the primary steps of user authentication. All the PC products can work on stationary desktops and servers, but buyer interests and greatest revenue opportunities come from systems that are movable.

Encryption may be invoked at the level of individual files, as is common on small mobile devices, or at the folder, partition, or full disk for larger systems. Users must answer a login challenge to gain access to data. The challenge may range from a simple PIN to a complex password, token or smart card, and may combine with biometrics. Competitive differences derive from different approaches to management, encryption strength, user authentication, policy management and value-added features, such as protection of information on removable media. Vendors must provide centrally managed access controls, lockouts and recovery methods.

Small mobile devices represent the largest number of platforms overall, but the largest profits are still made on Windows laptop/desktop platforms. Products restricted to Windows PCs may be considered, but the best rankings go to vendors that cross multiple platforms and OSs. MDP vendors increasingly offer secondary protection (bundled or stand-alone) for external port access controls and for external encrypted file storage, including network drives, external local drives and flash media. Thus, external media protection becomes a crossover function into stand-alone and specialized utilities (such as configuration management tools with device port controls, and trusted portable personality devices) that Gartner considers to be separate markets. Companies that sell port controls and external media protections as their only features, or as their main features, without meeting other core aspects of the MDP definition will not qualify for inclusion in this report.

Inclusion and Exclusion Criteria

Inclusion Criteria

Twenty-seven data protection vendors with MDP capabilities were notified of the annual survey. Fifteen passed the inclusion/exclusion criteria test and were included in the Magic Quadrant, according to the evaluation of these attributes:

- The vendor must have had products that were generally available in 2008 and in 1H09 for a sufficient length of time to attract market attention, and the products must meet all aspects of the definition of products in the market as set forth in this report. The vendor must offer products for use on PCs, because workstations represent most of the revenue for the market. Vendors that sell and/or source third-party encryption products are allowed; several vendors in this market license parts of their solutions, ranging from cryptographic modules to larger program components. A synchronization service running on a workstation or server to support a product that only runs on a handheld device does not qualify for inclusion.
- The vendor must generate sufficient client interest and inquiry to be noticed by Gartner security analysts. Analysts must also receive feedback from clients indicating that they are using the products.
- The vendor’s product must not be limited to a single or proprietary platform by restriction of an OS or hardware component.
- Gartner analysts have a generally favorable opinion about the company’s ability to compete in the market.
- The vendor should appear regularly on Gartner clients’ shortlists for final selection.
- The vendor should also appear regularly in other sources (such as publications and support forums) as a product that’s competitive with companies that are already qualified for this market.
- The vendor demonstrates competitive presence and sales to Gartner analysts. Competitive presence is improved greatly if the product is sold and supported in multiple countries, or, even better, in multiple geographies.
- Gartner analysts consider that aspects of the vendor’s product execution and vision are important enough to merit inclusion.
- Given the economic challenges of 2008 and 2009, the minimum revenue and seat thresholds have been kept at the prior report’s level. Seat sales in 2008 needed to total more than 125,000 seats, and 2008 revenue in the market must have been more than \$3 million. Exceptions may be granted if other inclusion factors merit consideration.
- The product must be commercially supported.

Seats sold by licensees, partners and others can only be counted once if reported. They will be attributed only to the original vendor if the licensee is not already included in this market study. OEM seats that are shipped without revenue may be attributed at a reduced percentage.

Exclusion Criteria

Vendors will not be included in the Magic Quadrant if the following conditions are not met:

- Vendors must return an annual request for information that is used to collect competitive and historical data within requested deadlines. Under limited circumstances, and at our discretion, we will estimate vendor status from a prior year's survey, but vendors that decline to report for two years in a row will be removed from ranking consideration.
- Vendors must report seat sales in a format requested by Gartner to allow for comparison. Under limited circumstances, and at our discretion, we may estimate unreported seats based on prior history, but vendors that decline to report for two years in a row may be removed.
- Vendors must report financial information in a format requested by Gartner to allow for comparison. In a mature market, financial data is desirable to make execution comparisons, and the majority of vendors report their results to Gartner. Wide variations in discounting and OEM contract values make estimations problematic. Other factors will be considered, including client interest, overall industry "mind share" and competitive behavior. Under limited circumstances, and at our discretion, we may estimate unreported financial performance based on prior history, but vendors that decline to report for two years in a row may be removed.

Vendors Considered for, but Not Included in, the 2009 Magic Quadrant

An assortment of vendors were queried, but either did not respond or missed critical response deadlines, or were not a match for the market criteria. The following vendors are noteworthy:

- Microsoft's encryption security products remain fragmented and are difficult to match to the inclusion criteria. Windows Mobile 6.1 supports core and removable memory encryption, but support for related security features is different, depending on which Microsoft platform is managing (that is, Exchange 2003, Exchange 2007 or System Center Mobile Device Manager). Furthermore, the supported features are different if ActiveSync is used on a non-Windows mobile device, and if ActiveSync is allowed, then it is difficult for companies to control which devices are synchronizing to the server (by default, only a valid user ID and domain password are required). Windows EFS has not changed since Windows 2000, so vulnerability concerns that were raised in past reports continue, particularly on XP platforms. Gartner sees little evidence for the adoption of BitLocker, and the situation will not improve until Windows 7 has a chance to build an enterprise presence. Microsoft has no common policy management platform for any of its encryption tools, which relegates them to the status of a collection of point

solutions that don't form a cohesive whole. Several ranked vendors provide common enterprise policy management and/or key management that work across all Microsoft platforms.

- Open-source projects, such as AxCrypt and TrueCrypt, offer free data encryption tools, but they are not commercially supported. Gartner monitors open-source projects and will consider future project distributions that provide commercial support.
- Seagate's encrypting drives are enabling technologies, rather than a complete solution; thus, they are not ranked on the Magic Quadrant. Buyers are best served by relying on third-party vendors in this market to manage keys, recovery and access policies for Seagate's drives. Vendors that support these drives will help you use the drive, if it is present, so you get the performance and reliability benefits; however, if you do not have the drive, then MDP vendors can use software encryption modules. In 2010, TCG's new open specifications for encrypted drives will take precedence as a cross-industry standard over Seagate's proprietary technology.

Added

Novell and Safend have responded to this year's survey and have met the inclusion criteria.

Sophos has entered the Magic Quadrant through its acquisition of Utimaco.

Dropped

ISC has not returned the survey for several years, and is pursuing security products outside the market definition for this Magic Quadrant. ISC's latest primary business development efforts are focused on its CertAgent, an X.509 v3 certificate authority product, and related certificate management tools. ISC still sells and supports its SecretAgent and SpyProof product lines, which have MDP capabilities, but the company's most recent role in MDP comes through a new partnership with Sophos, which can now sell SafeGuard under ISC's GSA SmartBuy status.

Secuware's entry into North America was, in Gartner's estimation, underfunded, and the company was missing milestones on the sales and product road map. Secuware scaled back its operations in North America and closed its U.S. office by year-end 2008. This was done without official notification to Gartner. Secuware's English-language website has not been updated since 2007. Secuware is working to develop sales channels to replace direct sales operations.

Utimaco was acquired by Sophos.

Evaluation Criteria

Ability to Execute

This market is well-established, and global pressure for data protection means that incumbent vendors can sell enough seats to keep their doors open. The recent economic slowdown has reduced the appearance of new companies; however, that is a good result because the large number of vendors already confuses buyers and limits the ability of incumbents to grow. Vendors

that learn to sell their products on the merits of ease of use and convergence with device management processes win the largest sales.

New products, new features and estimated sales in 1H09 are also considered in the final ranking. Unofficial road maps, pending contracts, future sales agreements and vague strategies do not significantly contribute to a vendor ranking or to inclusion in this research, but vendors that have official road maps and make consistent progress are recognized.

Product/Service compares the completeness and appropriateness of core data protection technology. This factor is critical in demonstrating that the vendor can generate market awareness.

Overall Viability considers company history and demonstrated commitment in the market, as well as the difference between a company's stated goals for the evaluation period and the company's actual performance, compared with the rest of the market. Growth of the customer base and revenue is considered.

Sales Execution/Pricing compares the strength of sales and distribution operations of the vendors, as well as the discounted list pricing for investments in seats ranging from fewer than 100 to more than 10,000. Pricing is compared in terms of first-year cost-per-concurrent active license seats, including the cost of the management console and all hardware and support. Buyers want demonstrable peace of mind more than they want bargains, and they respond more strongly to sales techniques led by case studies and return on investment (ROI) projections. In past years, the urgent need for protection meant that vendors in this market could charge up to hundreds of dollars per seat (obviously, lower prices are frequently negotiated). The arrival of EPP vendors in the market changes the rules because AV products have been heavily discounted. MDP buyers will expect deep discounting, and the average seat price can be expected to erode by as much as a factor of 10 during the next three years. This will stimulate market penetration, but challenge the survival of stand-alone and specialty vendors.

Market Responsiveness and Track Record and **Marketing Execution** are rated together as Marketing Execution. This criterion rates competitive visibility as a key factor, including which vendors are most commonly considered to be top competitive threats by each other, and which vendors respond most effectively during buyer RFPs.

Customer Experience is subjectively rated from client feedback to analysts; from opinions of Gartner analysts in security, network and platform research groups; and from vendor-supplied references, where needed.

Operations considers the ability of a vendor to pursue its goals in a manner that enhances and grows its influence in all execution categories. Operations is already considered in the other execution ranking categories (see Table 1).

Completeness of Vision

Vision is subjectively ranked according to a vendor's ability to show a broad investment in technology developments that predict user wants and needs.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	No Rating
Marketing Execution	Standard
Customer Experience	Standard
Operations	No Rating
Source: Gartner	

Companies that lead in vision typically own, license or partner on products in other security and configuration management markets. They must also demonstrate management features that make their products easy to integrate with enterprise directories, and to interoperate with other enterprise security and management systems.

Market Understanding and Marketing Strategy are ranked together as Marketing Strategy, assessed through direct observation of the degree to which a vendor's products, road maps and mission anticipate leading-edge thinking about buyers' wants and needs. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and by reading planning documents, marketing and sales literature, and press releases. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put plans in place, show that they are following their plans and modify their plans as market directions change. Also considered are the vendor's partnerships with other vendors in related endpoint security markets, including AV, anti-spyware, configuration management, authentication, device identification, virtual private networks, data encryption, gateway firewalls and others.

Sales Strategy examines the vendor's strategy for selling products, including sales messages, techniques, marketing, distribution and channels. This topic is considered to be in execution; it does not apply to product vision, which is ranked in terms of investment in functionality.

Offering (Product) Strategy is ranked through an examination of the breadth of functions, platform and OS support for the MDP client. R&D investments are credited in this category. Mergers that bring EPP vendors into the market have a strong impact on vision rankings for all vendors, because these vendors are driving the types of integration that Gartner considers to be strategic and competitive. Supported platforms are listed in the vendor comments. References to "Windows OS" refer to currently

supported full-end-user versions of the Windows XP, Vista and soon-to-be-released Windows 7 OS. Support may be available for older versions of Windows end-user platforms (9.x, 2000 and others) and servers. Vendors cited for support of Windows Mobile are ranked for support of Windows Mobile 6.0 and 6.1. Support may be available for other mobile OSs from Microsoft. Vendors cited for support of Apple are ranked for support of Mac OS X on Intel platforms. Support may also be available for PowerPC. iPhone support will be separately noted, if available.

Business Model takes into account a vendor's underlying business objectives for its products, and its ongoing ability to pursue R&D goals in a manner that enhances all vision categories.

Vertical/Industry Strategy considers a vendor's ability to communicate a vision that appeals to specific industries and vertical markets. The Magic Quadrant doesn't consider vertical markets as a distinctive ranking factor; therefore, this category is irrelevant.

Innovation takes into consideration the degree to which vendors invest in core requirements for the successful use of their products.

Geographic Strategy takes into account a vendor's strategy to direct resources, skills, products and services globally. All vendors are ranked in the Magic Quadrant for their performance as a whole, and within the frame of reference of Gartner clients; therefore, this category is not required (see Table 2).

Leaders

Leaders have products that work well for Gartner clients in small and large deployments. They have long-term road maps that follow and/or influence Gartner's vision of the developing needs of buyers in the market. Leaders make their competitors' sales staffs nervous and force competitors' technical staffs to follow their lead. Their MDP products are well-known to clients, and they are frequently found on RFP shortlists.

Challengers

Challengers have competitive visibility, market share, and financial and channel strengths that are better-developed than similar niche vendors. They have greater success in sales and mind share than similar niche vendors. Challengers offer all the core features of MDP, but typically their vision and road maps are narrower than the leaders, or are less likely to influence buying decisions. Challengers may have difficulty in communicating the effectiveness of their vision. For example, if a vendor has implemented features ahead of the demand curve that do not attract buyers, do not trigger new competitive responses from other vendors, and do not change the developmental course of the market, then its vision is not improved by those features.

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.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	No Rating
Marketing Strategy	Standard
Sales Strategy	No Rating
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	No Rating
Innovation	Standard
Geographic Strategy	No Rating
Source: Gartner	

Niche Players

Niche players offer products that suit many enterprise needs. A niche ranking is assigned when the product is not widely visible in competition, and when it is judged to be relatively narrow or specialized in breadth of functions and platforms, or, for other reasons, the vendor's ability to communicate vision and features does not meet Gartner's prevailing view of competitive trends. However, because the MDP market is a niche area in IT security, MDP niche players include stable, reliable and long-term players. Some niche players work from close, long-term relationships with their buyers, in which customer feedback sets the primary agenda for new features and enhancements. This approach can generate a high degree of customer satisfaction, but also results in a narrower focus on R&D than would be expected of a visionary.

Vendor Strengths and Cautions

Becrypt

Strengths

- Becrypt is a mature specialty company selling primarily in the U.K. and in North Atlantic Treaty Organization (NATO) countries. Although MDP seat sales are small, sales revenue is strong: Revenue was up 53% in 2008, and 30% growth is estimated for 2009. The company has positive cash flow and a favorable asset-to-equities ratio.
- Becrypt and CSC have announced a hosted virtual desktop service that's based on using Becrypt's Trusted Client, a component of its MDP suite, as a secure terminal. Becrypt is an exception to the SaaS story. Most vendors are generating only a few percent of revenue by SaaS, but Becrypt's SaaS revenue accounts for up to 20%.
- Becrypt has achieved FIPS 140-2; it also has Communications-Electronics Security Group (CESG) Assisted Products Scheme (CAPS) approved to Top Secret, and can export this level to major countries. Its CESG Claims Tested Mark (CCTM) certification is equivalent to CC EAL1.

- Supported platforms include Linux (Debian, SUSE and Ubuntu), Windows Mobile and Windows OS. Embedded support is provided for pluggable key management and replaceable Cryptographic Application Programming Interfaces.
- Bcrypt offers a good balance of MDP features, with a starting price that's about half the average across surveyed vendors.

Cautions

- Seat sales rates continue to be low for the time in business, and compared with the overall market, but the company has a baseline and market activity that are sufficient to continue its appearance in the Magic Quadrant. Revenue in other areas maintains Bcrypt's viability.
- Downward pricing pressure from larger companies — especially EPP vendors such as Check Point, McAfee and Sophos, which can afford to subsidize sales relationships — is a threat to Bcrypt's commercial market expansion.
- The company needs to develop aggressive and competitive marketing messages, combined with increased sales efforts outside Europe, to increase visibility.

BitArmor

Strengths

- BitArmor provides data control software that secures, tracks and controls sensitive data by attaching tags to the data to facilitate policy management decisions on laptops, removable media, servers and e-mail attachments. This approach presents a powerful strategic solution to data protection, because every file can directly assert its access policy.
- Company revenue, while small, grew more than 300% from last year and met the inclusion requirement.
- During 1Q09, BitArmor launched a clever No-Breach Guarantee campaign, offering a full refund to any company that experienced a data breach while using a BitArmor product.

Cautions

- The company must take further aggressive steps to improve visibility, and must move quickly to determine whether it can maintain a foothold in a mature, crowded market. It could be a valuable acquisition target.
- Seat sales were estimated to be within minimum range for inclusion for this report, although the company's method of counting licenses was not comparable to the norm and will be re-evaluated in 2010.

- Its methods of combining encryption and rights management are far advanced for the tactical buyer who is simply seeking an expedient means to make the auditor go away.

Check Point Software Technologies

Strengths

- Check Point is active in this market through its acquisition of Pointsec, and sells data encryption under Check Point and Pointsec brand names. LOB revenue for MDP was well above the average estimated for 2008. Seat sales in 2008 were above average, but not challenging to other companies that were ranked as leaders.
- The company tied with Sophos as the second most commonly cited competitive threat named by other vendors in the market (10 out of 15 vendor responses).
- Check Point is one of the few vendors to offer embedded support for visual passwords.
- Check Point provides some of the most extensive support for removable media policies and tracking, and meets all the criteria requested for core data encryption functions. It also provides extensive, best-in-class advice for travelers to foreign countries.
- Check Point has the following FIPS and CC certifications: FIPS 140-2 (all products); CC EAL4 Level 4 full disk encryption (FDE).
- Platform support is provided for Linux, Mac OS X, Palm OS, Symbian, Windows Mobile and Windows OS.

Cautions

- Check Point gave first integration priority between Pointsec and its EPP suite to the creation of a single end-user client, leaving the fragmented consoles for a later project. Gartner feels this choice was premature. Buyers are accustomed to running multiple security agents, and in this market, there is no resistance to purchasing separate agents. On the other hand, reducing the number of consoles involved in security policies is a tactical incentive with visible benefits for IT operations management.
- Execution was softened to a more conservative position, because the LOB and seat sales numbers reported in the 2009 survey were not as high as our estimates (made in 2008, when Check Point was not reporting results).
- Client feedback does not place this vendor at the head of the list. In Gartner's opinion, neither the brand names nor the vision is being effectively communicated. Clients that use products other than Check Point's are not predisposed to consider their MDP offerings. Check Point needs to take a lesson from Pointsec's past on how to market aggressively.

- Seat pricing for a broad platform of MDP functions is above average. Buyers expect EPP vendors to offer steep discounts, which is in keeping with the trend for AV and firewall products.

Credant Technologies

Strengths

- Credant continues to demonstrate that data-centric, data-policy-driven encryption products can compete in a market dominated by FDE vendors.
- Credant doesn't reconfigure the main drive or the OS; therefore, procedures for help desk, recovery, maintenance, patching and wake on LAN (WOL) are minimally affected.
- Credant has the following FIPS and CC certifications: FIPS 140-2 Level 1 and CC EAL3. It was included in the GSA's SmartBuy award.
- Credant's file-based architecture easily supports multiple private users on a shared device, and includes a roaming profile to allow guests to access private network directories from any system hosting a Credant agent.
- Credant provides extensive, best-in-class advice for travelers to foreign countries.
- Platform support is provided for Palm OS, Symbian, Windows Mobile and Windows OS. Embedded system support includes the ability to manage BitLocker, EFS, Seagate's encrypting drives and the TPM. Credant had a strong early partnership with Intel for integration with vPro.

Cautions

- Credant's revenue increased in 2008, but not at a rate that would be historically expected with a 26% increase in customer base. The company's three-year cumulative seat sales are above average, but seat sales for 2008 did not continue the momentum. Credant's overall performance earned a somewhat-lower execution than in 2008.
- Credant has struggled with a lack of competition. Other vendors with data-centric encryption have offered less-sophisticated policy management, and if their products were seen first, then they could deflect buyers from taking a closer look at Credant. Two factors will help, but require time to develop. First, increasing interest in removable media protection forces buyers to compare products with data-centric protections, which is Credant's core expertise. The second factor is the TCG announcement of standard specifications for storage encryption. As MSP vendors turn to managing hardware encryption, the story of FDE in software becomes moot.

- Buyers occasionally encounter operational problems that are attributed to programming quirks in their system software and applications, which are different in nature than the occasional stability problems reported by clients that install FDE products. These problems are easy to resolve, but require better reseller training.

GuardianEdge Technologies

Strengths

- Overall growth continues to be strong into 2009 — about 30% over 2008, which continues a surge that began in 2006 after the data breach at the U.S. Department of Veterans Affairs. Seat sales for 2008 were nearly three times the average of vendors reporting in this study. GuardianEdge is proof that smaller, dedicated MDP vendors can directly challenge larger companies with broader offerings.
- GuardianEdge's OEM relationship with Symantec has contributed to its success in 2008-2009, and to its rating in this report. Symantec waived an opportunity to be listed in this report so that the execution credit would accrue to GuardianEdge.
- GuardianEdge provided a superior set of examples of system-generated audit reports.
- GuardianEdge has the following FIPS and CC certifications: FIPS 140-2 and CC EAL4+. It was included in the GSA's SmartBuy award.
- Platform support is provided for iPhone, Palm OS, Symbian, Windows Mobile and Windows OS.

Cautions

- The relationship with Symantec is puzzling to buyers. Many companies that own or consider Symantec products are unaware of the relationship, and some have found themselves bidding on the same product from different sources.
- GuardianEdge's Data Protection Platform is very complete, and will be quoted at a relatively high per-seat price prior to negotiation.

McAfee

Strengths

- McAfee has been the most commonly named competitive threat (12 out of 15 vendor responses) for two years in a row.
- Revenue in the LOB containing data encryption products is the second highest reported among responding vendors. Non-OEM seat sales for MDP were the highest reported, and OEM sales were the largest reported.

- McAfee is the only vendor in the survey that described a method to enforce keyword scanning content-based encryption on files sent to removable media. In addition, it offers extensive write-blocking policies by device type.
- The Total Protection for Secure (ToPS) Business agent performs continuous health checks to predict and avoid encryption system failures.
- McAfee has the following FIPS and CC certifications: FIPS 140-2 and CC EAL4. It was included in the GSA's SmartBuy award.
- Platform support is provided for Linux, Palm OS, Windows Mobile, Symbian, and Windows XP and Vista.

Cautions

- Console integration between ToPS and other McAfee products needs to be completed.
- McAfee offers an optional, non-FIPS-certified cryptographic algorithm at installation. This was included for backward compatibility and is not the default, but if the non-FIPS option is chosen, then it forces all agents in the enterprise into a non-FIPS operational mode. McAfee's dashboard and auditor report does not indicate that monitored devices are in FIPS or non-FIPS mode.
- The dashboard also doesn't report the difference between a client device with a fully enrolled and authenticated user, and a client device in which the user has not completed his or her enrollment (called preboot authentication [PBA] pass-through mode). PBA pass-through mode makes it easy to generate a new workstation from a standard image. The reporting distinction is urgently needed because, in pass-through mode, the system does not present an authentication challenge, and, therefore, is exposed.

Mobile Armor

Strengths

- Mobile Armor offers its full suite of products for purchase or as SaaS, and had 15 SaaS clients as of January 2009.
- Mobile Armor was the first MDP vendor to offer network-aware PBA. It can process system updates without unlocking the hard drive or starting the host OS. This is particularly valuable to companies that want to process unattended updates.
- Mobile Armor provided a superior set of examples of system-generated audit reports.
- Mobile Armor has the following FIPS and CC certifications: FIPS 140-2 Level 2, CC EAL4+ and U.S. National Security Agency (NSA) Communications Security (COMSEC) Suite B. It was included in the GSA's SmartBuy award.

- Platform support is provided for Mac OS X, Research In Motion (RIM), Symbian, Linux (Red Hat Enterprise Linux 5 and SUSE), Windows Mobile and Windows OS. Embedded support is provided for Seagate encrypted drives, and the product is ready for new TCG-compatible drives.

Cautions

- The major source of growth for Mobile Armor stems from military agencies. Mobile Armor provides a broad suite product at a schedule price that's well below the average, but it lacks the resources to build visibility. Aggressive and competitive sales techniques and more active reseller partners are still needed to get Mobile Armor recognized by potential buyers in larger, nongovernmental markets and geographies outside North America.
- Seat sales are at the inclusion threshold after three years of selling openly in the market, and they need to be seen to grow significantly for inclusion in 2010.
- Although Mobile Armor provides a broad suite product at a price that's well below average, downward pricing pressure from larger companies — especially EPP vendors such as Check Point, McAfee and Sophos, which can afford to subsidize sales relationships — is a threat to Mobile Armor's commercial market expansion.

Novell

Strengths

- By its acquisition of Senforce Technologies, Novell gained a best-in-class firewall with abilities to control the use of device ports and removable media. This led to the release of the ZENworks Endpoint Security Management (ZESM) product, which also implements main drive file and folder encryption that can be used for comprehensive data protection.
- ZESM is tightly integrated with ZENworks, thereby making it an easy choice for Novell-centric IT shops.
- Novell has the following FIPS and CC certifications: FIPS 140-2 and CC EAL4+.
- Platform support is provided for Palm OS, RIM, Windows Mobile and Windows OS.

Cautions

- Novell is not recognized as a competitor in this market by other MDP vendors or Gartner clients. Buyers seem likely to buy ZESM as a point solution for removable media protection. However, execution in terms of ZESM seat sales and LOB revenue is strong enough to earn Novell a borderline challenger ranking.

- Novell has limited experience with data-centric protection and has not built a competitive business case to be more than a specialty vendor.

PGP

Strengths

- PGP managed to grow direct sales revenue of 30% in a tough economy, and reports 26 quarters of positive growth as of 1Q09. Visibility drives sales opportunities, and clients frequently ask about PGP. A pay-as-you-go SaaS was added in 2008, but is not yet generating significant revenue. Also, since last year's report, PGP has cultivated a reseller deal with IBM.
- PGP's broad commitments to integration and interoperability with adjacent security market players and shared key infrastructures across multiple PGP products, including e-mail and instant messaging, contribute to a strong vision ranking.
- PGP has the following FIPS and CC certifications: FIPS 140-2, CC EAL4+ and U.K. CAPS.
- Platform support is provided for Linux (Red Hat, Fedora, SUSE), Mac OS X, RIM (e-mail only), Unix (Solaris, HP-UX, AIX), Windows Mobile and Windows OS. Embedded system support includes the Intel vPro and Anti-Theft Technology — Data Protections (AT-d), as well as TPM.
- PGP provides extensive, best-in-class advice for travelers to foreign countries.

Cautions

- PGP needs to develop deeper alliances and licenses with EPP vendors to hold up against the EPP vendors that are setting the future standard for vision in this Magic Quadrant. PGP would also make an attractive acquisition target.
- Its open-source heritage should be further developed for sales and marketing clout.

Safend

Strengths

- Safend resells removable media protection to several vendors in the Magic Quadrant, and is qualified for inclusion based on sales revenue and non-OEM seat sales.
- Safend has a feature to expose a single application on a locked PC. This could be used, for example, to allow a courier to circulate a tablet PC with a sign-off form on display, while otherwise maintaining encrypted access to the system and underlying data.

- Certifications include FIPS 140-2 Level 1 and CC EAL2.

- Platform support is provided for iPhone, Windows Mobile and Windows OS.

Cautions

- Safend's price for a suite of MDP features with full management is less than the average, but its relatively low visibility is a barrier.
- Safend relies too heavily on OEM partners because they limit revenue potential and already sell competitive products. To grow as a stand-alone player, Safend needs to cultivate direct resellers.
- Lockout functions need to be added soon, including remote lock/wipe and lock after failed login attempts.

SafeNet

Strengths

- SafeNet is authorized to develop and sell U.S. government Type 1 (classified) encryption products. Approximately 50% of LOB revenue comes from Type 1 products.
- SafeNet sells an optional hardened key storage/key escrow appliance server to provide the maximum defense of system recovery data.
- SafeNet has the following FIPS and CC certifications: FIPS 140-2-2 and CC EAL4. It was included in the GSA's SmartBuy award.
- Platform support has been expanded to provide for iPhone, Palm OS, RIM, Linux, Macintosh, Unix, Windows Mobile and Windows OS. Additional support is available for redundant array of independent disks (RAID), which makes this product appealing for servers.

Cautions

- SafeNet currently generates only a few inquiries in the MDP area from Gartner clients — end users and other vendors — and lacks visibility in nongovernment markets. It is not considered a competitive threat by any company that Gartner tracks in the market. Aggressive and competitive sales techniques and more nongovernment reseller partners are still needed to get SafeNet recognized by potential buyers in other industry segments.
- SafeNet should expand its write blocking policy beyond basic port monitoring to include utilities such as third-party CD/DVD burners and named applications (that is, Application A is allowed to write data to the Universal Serial Bus [USB] port and optical drive, while all others are denied).

Sophos

Strengths

- Through its completed acquisition of Utimaco, Sophos has created a combined company that can challenge McAfee. The cultures of the companies were compatible and friendly, and the new road map is impressive. Sophos tied with Check Point as the second most commonly cited competitive threat named by other vendors in the market (10 out of 15 replies). In 2008, revenue in the MDP LOB was almost twice the estimated average, growing 18% over 2007. The proportion of LOB revenue in the U.S. market dropped in favor of stronger sales in Europe, but is still a significant and respectable amount. In 2008, seat sales were above average, similar to Check Point, but not challenging to GuardianEdge and McAfee.
- Sophos provides extensive support for removable media policies and tracking. It also provides comprehensive advice for travelers to foreign countries.
- Sophos has the following FIPS and CC certifications: FIPS 140-2 and CC EAL4. Sophos has arranged to be listed on the GSA's SmartBuy program through a clever arrangement with ISC, which now acts as its reseller.
- Platform support is provided for Palm OS, Symbian, Windows Mobile and Windows OS. Embedded system support includes the ability to manage BitLocker, Seagate's encrypting drives and the TPM. It is also integrated with Intel vPro and has a long-term relationship with Lenovo, which includes integration with Lenovo Rescue and Recovery.

Cautions

- North American market penetration was difficult for Utimaco prior to the acquisition, and is also a challenge for Sophos. Neither company gives the other a better foothold, but Sophos has more money and more distribution potential to bring SafeGuard products to new buyers.
- Sophos' execution on the strategic vision for the combined company has been delayed by the time and complexity of European acquisition laws and regulations. However, the requirements are now fulfilled, operational integration of the two companies is complete, and the strategy and road map execution are well under way.
- Gartner clients' recognition of Sophos on shortlists outside of AV is infrequent and not on par with its strengths. The Utimaco name was finally gaining ground before acquisition.

Sybase iAnywhere

Strengths

- Parent company Sybase enjoyed strong earnings in 2008 and shows no sign of slowing down in 2009. Overall revenue

increased 14%, and 1Q09 was the company's strongest quarter in history. LOB revenue was the highest reported, but is a lot more than MDP; it includes a wide range of products that fall under the Sybase iAnywhere and Afaia brands.

- Sybase iAnywhere offers the most complete set of fully integrated configuration management and MDP features owned by a single vendor. It has been promoted to visionary because configuration management capabilities are increasingly recognized by buyers.
- Sybase iAnywhere provides its own embedded theft tracing via IP address, and also traces smartphones through text message monitoring.
- Sybase iAnywhere has the following FIPS certification: FIPS 140-2 Level 1 for all products.
- Platform support is provided for iPhone, Palm OS, RIM, Symbian, Windows Mobile and Windows OS.

Cautions

- Seat sales in the MDP market are remarkably low, given the billion-dollar investment power of parent company Sybase. This is partly due to a preferential interest in ignoring the PC market, where seat values are higher, in favor of the handheld market, where sales and revenue are more challenging. Sybase iAnywhere is recognized in this report for that challenge; however, at the same time, its execution compared with the peer group is weakened.
- Sales were below market average for four years through 2008. However, in 2008, Sybase started to grow handheld encryption sales at a notable rate.
- Sybase iAnywhere has provided no specific direction for supporting embedded hardware (such as Intel vPro, TPM and encrypting hard drives).
- The breadth of the management platform is not driving sales, so vision and execution are hampered when, in fact, Sybase iAnywhere should be competitively challenging and outperforming the EPP vendors that have entered this market. Given its strong financial position, parent Sybase should consider acquiring an EPP vendor.
- The company is behind the market norm with regard to access control policies for data on removable media.

Wave Systems

Strengths

- For several years, Wave Systems has offered a self-contained solution for managing keys, reporting and recovery for PCs that are equipped with Seagate encrypting drives. It also supports

Samsung/Opal-compliant encrypting solid state drives on several business notebook models. In addition, the company supports TPMs from many manufacturers.

- Wave was early in line to support the new TCG specifications that were announced in January 2009. A new supply of manageable drives based on TCG specifications could expand Wave's sales prospects in 2010.
- A dedicated key management server helps companies back up keys to an existing platform, and migrate keys to new platforms for recovery or migration.
- A stand-alone version of the product is included on qualified Dell PCs, and is upgradable to an enterprise managed platform. Additional bundling is available with motherboards from Intel and PCs from NEC (in Europe), and from Gateway, MPC, ASI, and Acer. Embedded system support includes Intel vPro, TPM, Seagate encrypting drives and TCG-compatible drives.

Cautions

- Wave Systems added management for SafeNet ProtectDrive in support of FDE without hardware encryption, but its main value in the MDP market through 1H09 was bound to Seagate's encrypting drives. Wave's strategic value proposition will expand as TCG hardware encryption becomes generally available in magnetic, solid-state and flash disk products. However, other vendors in this market are also betting on the TCG designs.
- Wave does not possess FIPS or CC certifications that are comparable with other software vendors in this report, nor do the encrypting drives it supports. Policies that evaluate and qualify encrypting drives for use in government agencies have been prepared by the NSA under the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11.
- Wave Systems generates revenue that is below the median and far below the average, given the large numbers of OEM seats that it supplies. Primary distribution is performed by an OEM-embedded stand-alone client on selected PC platforms. Users can deploy the client without purchasing Wave Systems' enterprise management, and there is only a limited sales mention on the Dell website configuration page (for example, to attract users to a larger purchase).
- The company should develop additional sales channels to promote its full enterprise solution. The company's market impact is only fractionally considered because stand-alone OEM seats are not trackable and do not advance the goals of enterprise managed data protection. The customer incentive to purchase the managed versions of Wave OEM products will increase with the release of new encrypting drive models, and will be re-evaluated in 2010.

WinMagic

Strengths

- WinMagic managed to grow its 2008 revenue nearly 30% over 2007. The company is profitable and debt-free.
- WinMagic has drag-and-drop support for many popular data-copying applications, such as CD and DVD burners.
- A feature called the Geo-Fence uses IP address information to decide how to execute preboot authentication based on a geographic boundary (such as a continent, country or state).
- WinMagic has the following FIPS and CC certifications: FIPS 140-2 Level 2 and CC EAL4. It was included in the GSA's SmartBuy award.
- Platform support is provided for Linux, Mac OS X, Windows Mobile and Windows OS. Embedded system support includes Seagate encrypting drives and TPM, and the product is ready for new TCG-compatible drives.

Cautions

- Recognition of WinMagic and the appeal of its innovative features are under-reported among Gartner clients who pose inquiries. For example, its early innovative methods to catalog legacy encryption keys and aid archival recovery generally have not caused Gartner clients to revise their shortlists to prioritize WinMagic.
- Sales and emphasis continue to lean toward the high-security specialty markets, thus earning WinMagic a niche player ranking.
- WinMagic must learn how to market the product to expand awareness and appeal to the majority of users that resist strong security products, and, in anticipation of the changes caused by EPP vendors in the market, it should seek an aggressive sales alliance with a major EPP vendor.
- WinMagic needs to be seen and mentioned more often outside of booths at security conferences, and must find better ways to position itself as an enterprise solution instead of a technology provider. Having good technology is not enough to prevail in an increasingly competitive market.

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 website, 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.