Mobile data protection products secure data on storage systems in notebooks and removable media, but also work on desktops and servers. Buyers want common protection policies across multiple platforms, minimal support costs and proof that data is protected.

**Market Definition/Description**

In the mobile data protection (MDP) market, Gartner tracks software utilities that enforce confidentiality policies by encrypting data, and then managing access to that encrypted data on the primary and secondary storage systems of end-user devices. The market primarily serves devices that are mobile in design and use case, even though the market originated earlier than laptops. Storage systems include the primary boot drive of a workstation and removable devices used for portability. Storage technologies affected by MDP products include magnetic hard-disk drives (HDDs), solid-state drives (SSDs), flash drives and optical media. Some vendors may be able to set policies for network storage, but that is not core to the current definition.

A typical MDP product consists of a central console that controls client installations and activations, pushes data protection policies, interfaces with the help desk, acts as a key management facility, and generates alerts and compliance reports. A local endpoint agent is provided to operate encryption for the target workstation/device, plus a utility to be copied to removable media to manage password access. These agents can respond to central server directives, or can take direct actions to lock or wipe a device that falls out of compliance.

MDP products provide active services bound to the OS and basic input/output system (BIOS) services of their host platforms, so they can control primary storage input/output and insert themselves in the primary steps of user authentication. With few exceptions, MDP products are capable of providing all encryption/decryption processes as software services to the OS. New developments have allowed MDP products to offload part or all of this work to hardware elements, including the CPU and drive controller. However, MDP cannot simply be replaced or made obsolete by hardware components. A central MDP management framework will always be the focal point for encryption policy management, key access and storage, system recovery, and audit reports.

Encryption may be invoked at the level of individual files or at the folder, partition or full drive, depending on the use case. 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 use biometrics. Competitive differences derive from various approaches to management, encryption
strength, user authentication, policy management and value-added features, such as the protection of information on removable media and breadth of platforms supported.

The market is called "mobile data protection," because the primary buying decision has always centered on portable devices that cannot rely on traditional physical security. However, the technology works well and has value on nonmobile systems, such as desktops and servers, and most vendors obtain a portion of the income from stationary workstations.

About two-thirds of MDP revenue is generated from sales to support notebook (laptop) computers based on the Windows OS, but buyers are also increasingly looking for Mac OS X and Linux support. Additional consideration will go to vendors that cross multiple platforms and OSs. Security and management support for smartphones and tablets running nonworkstation OSs is being satisfied by a different market called mobile device management (MDM) and forms the basis for the Magic Quadrant for MDM software. Several vendors in this report have MDM products and services, but buyers give overwhelming feedback to Gartner that they treat the purchases separately.

Magic Quadrant

Figure 1. Magic Quadrant for Mobile Data Protection

Source: Gartner (September 2012)
Vendor Strengths and Cautions

Check Point Software Technologies

Check Point Software Technologies built its MDP investment through the acquisition of Pointsec, an influential pure-play encryption provider. Platform support is provided for Windows 2000 through Windows 8, Mac OS X and Linux. Mobile device support for iOS, Android OS and various legacy platforms, including Windows Mobile 6.5, is provided via a separate product, Check Point Mobile, which also extends VPN and container encryption that are managed under MDP. Check Point has U.S. Federal Information Processing Standards (FIPS) and Common Criteria (CC) certifications for FIPS 140-2 Overall Level 1, CC EAL2 and CC EAL4+.

Strengths

- Check Point has a strong position in remote access for workstations and smaller devices, providing a customer base that potentially would be interested in other security technologies for those same platforms. This includes an early release of smartphone data loss prevention (DLP) agents.
- Its protect-on-LAN policy automatically wipes a system that is used outside of predefined networks.
- Check Point’s dedicated secure hardware device called Go, formerly Abra, supports specialized high-security use cases and portable Windows applications.
- Check Point has added client-side, event-driven training prompts to better guide users regarding data movement policies onto removable media. The administrative interface’s readability has also been augmented with natural-language views of policies.

Cautions

- Check Point’s current implementation for software encryption on USB flash drives requires initial activation (a one-time step) on a Windows system. Buyers should account for this as a possible operational compatibility issue in mixed Windows/Mac organizations.
- Buyers with long memories of encryption challenges on older Windows platforms might miss opportunities, unless they review Check Point’s newest generations of products. This is a side effect of the long time that Check Point and Pointsec products have been in the market.

Credant

Credant is one of a few companies in the MDP market that successfully fought the bias for full-disk encryption (FDE) for years by offering superior function in file- and folder-based protection. Credant now also offers FDE. Platform support is provided for Windows XP through 64-bit Windows 7 and Mac OS X. Windows 8 support is planned to be available within 45 days of its release. An MDP-managed version for iOS and Android OS is planned for future release. Embedded system support includes Seagate and Trusted Computing Group (TCG) encrypting drives, and the Trusted Platform
Module (TPM). Credant has certifications for FIPS 140-2 Level Overall 1 and CC EAL3, with CC EAL4+ in final review.

**Strengths**

- Gartner receives indications from client inquiries that Credant’s sales are being successfully leveraged through Dell and LANDesk. The company is profitable and has long-term stable investors. Dell integrates Credant FDE with the Dell BIOS. This configuration can reach FIPS 140-2 Level 3 by adding the Dell Hardware Encryption Accelerator based on STMicroelectronics' HardCache.

- Credant continues to attract buyers that do not want to replace the boot process, and prefer minimal interference with normal OS operations and conventional help desk procedures. Credant’s method is appropriate for scaling large numbers of users on multiuser systems, with roaming profiles and unattended wake-on-LAN updates.

- Credant provides basic management for BitLocker to harden the default configuration, and to enhance key management and user recovery, as well as to stop administrative users from turning off encryption.

**Cautions**

- Seat sales dropped during the survey period, but are well within the inclusion criteria and are supplemented by customers who layer Credant’s removable media encryption on systems using other MDP products.

- Many prospective buyers are completely unaware of Credant’s approach to encryption and overlook their options in favor of a default assumption to use FDE. This is especially true of multiuser and bring your own device (BYOD) workstation configuration opportunities.

**McAfee**

McAfee is a long-term player in the MDP market. Integration of MDP into its Total Protection suites and McAfee ePolicy Orchestrator (ePO) management architecture is among the most successful by an endpoint protection platform (EPP) vendor, and has set the bar for MDP market performance. Platform support is provided for Windows XP through Windows 7 and Mac OS X. Windows 8 support will be released 30 days after general availability. MDM support is offered in a separate product, McAfee Enterprise Mobility Management, for iOS, Android OS and legacy platforms, including Windows Mobile 6.5. Embedded support includes Intel Advanced Encryption Standard New Instructions (AES-NI), TCG encrypting drives, TPM and Extensible Firmware Interface (EFI). McAfee has certifications for FIPS 140-2 Overall Level 1 and CC EAL4. It is the first MDP vendor at the time of publication to receive FIPS 140-2 certification for use of the Intel AES-NI CPU-accelerated technology.
**Strengths**

- Gartner client inquiries strongly associate McAfee’s MDP products and EPP products. Seat sales for McAfee’s MDP are the highest in the survey, combined with the highest attributed revenue. McAfee tied for the highest competitive threat rating in 2012 by its peer group.
- McAfee provides native content filtering in the MDP product to conditionally block data by type or contents. Within the Total Protection for Data suite, host DLP, location-tagged data and device control are included standard.
- On Windows and Mac OS X platforms, the Endpoint Encryption Go (EEGO) utility, a dedicated tool for compliance assessment, performs a thorough analysis on systems to predict and prevent disk encryption installation failures. EEGO can run continuously to provide future failure warnings.
- A Windows OS refresh tool is supported that allows automated, data in place, noninvasive Windows migrations with Microsoft-provided deployment tools.
- Standard maintenance support is included at no extra charge.

**Cautions**

- MDP revenue growth has slowed because MDP is increasingly bundled at a discount in McAfee suites. Buyers seeking stand-alone MDP can purchase it, but will find that new offers are geared toward EPP migration.
- McAfee ePO Deep Command is pursuing an ever-deeper integration with Intel Active Management Technology and other hardware-assisted maintenance features, which are exciting on the surface but are not indicated as high priority for MDP buyers. This is an interesting vision that will not necessarily enhance buyer value on legacy workstation platforms.
- McAfee’s software-based secure vault for USB flash drives presents an Explorer-like interface but doesn’t fully support Windows drag-and-drop file operations when used in off-site mode on unmanaged workstations. References report that this limitation causes user confusion about how to open and save files, and can generate help desk calls, as well as extra copies of files that could be left in unsecured storage in BYOD use cases.

**Microsoft**

Windows 7 BitLocker and BitLocker To Go are considered a product family for ranking purposes, because buyers consider it to be an alternative to standing products in this market. Under Windows 8, hardware encryption support will be offered for the first time, based on a new family of TCG-compliant drives designed for Windows compatibility. Windows 8 encryption for workstations and mobile devices will be investigated in future reports.
**Strengths**

- Gartner client interest in BitLocker has grown in the context of Windows 7 migration, and Microsoft is considered a significant competitive threat by other MDP vendors. Execution is raised slightly, owing to lack of hard evidence of competitive displacement.
- BitLocker activation is extremely simple, and users will not experience a long setup time for the hard drive to encrypt.
- As an embedded Windows 7 process, BitLocker efficiency is very good, and users experience minimal performance effects.
- Microsoft BitLocker Administration and Monitoring is now available as part of the Microsoft Desktop Optimization Pack for Software Assurance. Clients are reporting that it is facilitating deployments with simpler provisioning, auditing and key management.

**Cautions**

- Buyers should consider ways in which BitLocker interacts with other Microsoft products. For example, on a drive where a startup PIN is used as a preboot challenge, DirectAccess cannot start until the drive is unlocked.
- On a multiuser workstation, selective user account encryption and document protection may require supplemental use of Microsoft’s Encrypting File System and Rights Management Services, neither of which share policies with BitLocker. This results in multiple layers of available protection that may need to be managed separately.
- A TPM chip must be present. Otherwise, the user must carry his or her access key on a flash drive or remember a long number string.
- There is no expiration or update mechanism for a user’s PIN code. Operating in FIPS 140-2 mode, BitLocker administration and recovery features are restricted, and administrative users can still deactivate BitLocker. Buyers needing FIPS-level operation should investigate potential function gaps in any product that runs in multiple modes — not just BitLocker.
- Windows 7 limits BitLocker system drive and flash drive activation to two versions, Ultimate and Enterprise — neither of which would be common for users who participate in "bring your own PC to work" programs. Enterprises should anticipate early pressure to support Windows 8 BitLocker on BYOD systems, even if their current plan is to stay with Windows 7. Flash protection is limited to full-volume encryption, read-only on Vista and XP, and unreadable on Mac OS X or Linux.

**Novell**

Novell, which is now doing business as part of the Attachmate Group, offers software file-based encryption and support for Seagate self-encrypting drives through the Novell Endpoint Protection Suite (NEPS). TPM support is also available. NEPS doesn’t provide anti-malware protection; however, it will verify the presence and operation of the user’s choice of anti-malware products. Platform support is provided for Windows 2000 through Windows 7, Mac OS X and Linux (Red Hat...
and SUSE). Additional support is provided for iOS, Android OS, Windows Mobile 6.5 and Windows Phone 7. Windows 8 support is planned for release 90 days after the availability of Windows 8. Novell has certification for FIPS 140-2 Overall Level 2 and CC EAL4+.

Strengths

- NEPS can be deployed stand-alone or through a common configuration management console shared with ZENworks.
- Location awareness capabilities enable dynamic adjustments to the encryption system for roaming users. For international travelers, this could include changes to encryption key length and type based on country rules and compliance requirements.
- NEPS shares Java and Visual Basic scripting support with ZENworks that enables real-time data protection decisions to be tied to event-driven changes in a client workstation.
- After a dip in seat sales and not participating in last year’s Magic Quadrant survey, Novell’s calendar-year 2011 seat sales meet a strong average and are well above the median in keeping with a stable Niche Player.

Cautions

- Novell tends to sell its MDP technology into its existing customer base. Therefore, buyers composing MDP RFI lists may consider it a specialty product. Client references tend to associate NEPS with the configuration management market, rather than with MDP.
- NEPS is not configured to generate standard compliance reports; however, administrators can compose their own reports.
- Novell does not have a methodology to support wake-on-LAN maintenance updates on an encrypted workstation.
- Gartner client feedback, a scarcity of publication references or reviews, and lack of peer vendor reaction continue to signal a lowered standing in competitive market presence.

Secude

SAP acquired Secude’s Secure Login and Enterprise Single Signon assets in 2011, as part of a plan to augment SAP products with these capabilities. Secude remains an independent company continuing development on its legacy MDP product, FinallySecure Enterprise, and developing a new file-based MDP product, SecureFolder Enterprise. Platform support includes Windows XP through 64-bit Windows 7, Windows 8, Mac OS X and Linux versions, as well as TCG encrypting drive support, are in prerelease testing. Embedded support includes Seagate-encrypted drives and TPM. Secude encryption is certified to FIPS 140-2 Overall Level 1.
Strengths

- Secude does the majority of its business in a subset of EU countries with a few partners, making it an attractive niche provider in limited geographies.
- Secude is designed to integrate into a company’s existing management framework, rather than to replace it or run stand-alone.
- Novell is obtaining FDE technology from Secude, providing a new opportunity for visibility.

Cautions

- Prospective buyers should note that Secude’s seat sales during the study period are below the threshold for new inclusion, but the company is carried forward based on prior inclusion and because its products are viable on specification.
- The products sold to SAP in 2011 would have made FinallySecure Enterprise more competitive for enterprise MDP use cases.
- Secude does not have competitive presence in related security markets identified to be contributory to MDP growth, such as EPP or DLP.

Sophos

Sophos is a long-term EPP player that successfully integrated the Utimaco SafeGuard MDP offering. It continues to have strong European presence in EPP and MDP. Platform support is provided for Windows 2000 through 64-bit Windows 7, Mac OS X and Linux. Sophos Mobile Control and Sophos Mobile Encryption are separate products supporting iOS and Android OS devices. Embedded system support includes TPM, TCG encrypting drives, Intel vPro and EFI. Windows 8 support is slated for a release that will coincide with Microsoft’s Windows 8 release. Sophos has certifications for FIPS 140-2 Overall Level 1, CC EAL3+ and EAL4.

Strengths

- Client satisfaction with SafeGuard, as well as progress on the company’s development road map, is favorable and counts strongly toward its leadership ranking.
- An optional feature in version 6, SafeGuard FileShare, extends Sophos encryption to file servers and cloud storage at an additional charge.
- Sophos is easy to implement in a file-based mode (not FDE) to support private files on multitenant workstations supporting large numbers of users.
- Sophos integrates content-aware DLP into its client to help decide when to enforce encryption on information being written to external devices.
- When SafeGuard is installed as FDE in a VM, it does not allocate the full disk size upfront. This helps reduce the support burden for source and backup holographic versatile disc (HVD) images stored on servers.
Cautions

- Sophos’ market presence doesn’t line up with brand awareness, which remains limited, especially in feedback from clients in North American markets. Most Gartner MDP inquiries and bid reviews do not mention Sophos as a finalist.
- Buyers are likely to be unaware of new features, and may miss opportunities or buy other products, because Sophos is not assertive in efforts to communicate and to keep customer relationships up-to-date.
- Windows Client only supports Unified Extensible Firmware Interface (UEFI) via BIOS emulation. Full native UEFI preboot support is pending.
- Functional parity between versions for Windows and Mac OS X needs improvements (for example, in support for file-based encryption).

Symantec

Symantec acquired PGP and GuardianEdge in 1H10. The products will be rebranded at year-end under the single name Symantec Drive Encryption (SDE) — formerly PGP Whole Disk Encryption. Symantec has certifications for FIPS 140-2 Overall Level 1, CC EAL2 and CC EAL4+. Symantec has very broad MDP platform support, including Windows 2000 through 64-bit Windows 7, Mac OS X, Linux and Unix. Small devices are supported by a separate MDM product, Symantec Mobile Management. Embedded system support includes TPM, Intel vPro and EFI. Windows 8 support is planned for 1H13.

Strengths

- Symantec’s reputation and global reach continue to push sales forward. The company has a huge installed base into which it can sell new and upgraded MDP. Seat sales were strong for the study year and are increasing.
- Symantec tied for the highest competitive threat rating in 2012 by its peer group.
- The capabilities obtained from the acquisitions of PGP and GuardianEdge mean that Symantec can address nearly all client scenarios and approaches for MDP.
- The PGP Viewer facilitates access to encrypted email on Apple iOS mobile devices by extending the management of MDP policies.

Cautions

- Symantec’s road map to merge the best capabilities of SDE based on PGP and Symantec Endpoint Encryption-Full Disk (SEE-FD) based on GuardianEdge products into a single offering with common management is still not manifested into shipping products two years after being announced at the time of the acquisitions.
The fact that Symantec found it necessary to maintain two separate offerings with fundamentally different architectures and design approaches drove some Symantec customers to seek alternate third-party solutions for MDP.

Gartner is still receiving reports of client concerns over support in 2012, although at a much lower rate than previously experienced. Clients are advised to assess support options and to discuss their architectural details with a qualified installer before implementation.

Symantec has not yet integrated its MDM offerings into the SEP management console. MDM can be managed from Altiris.

Trend Micro
Trend Micro completed the acquisition of Mobile Armor in 2011. It now offers FDE, file and folder encryption, and a hardened and encrypted USB flash drive. Platform support is provided for all versions of Windows from 2000 through Windows 7. Separate MDM products, Trend Micro Mobile Security and Hosted Mobile Security provide management for iOS, Android OS and Windows Mobile 5+. Embedded support is provided for Seagate-encrypted drives, TCG encrypting drives, TPM, Intel vPro, Intel AT and EFI. Windows 8 support is planned for release in conjunction with the availability of Windows 8 SP1. Trend Micro has certifications for FIPS 140-2 Overall Level 2, CC EAL4+.

Strengths

- Trend Micro’s acquisition brings new viability to a good-quality suite of encryption products. Full policy integration is in this year’s road map. Encryption status can be monitored in Trend Micro’s Control Manager today.

- Trend Micro has developed Installation Advisor, a dedicated tool that automatically performs disk and OS health checks before installation to prevent installation failure, and also evaluates application compatibility.

- Buyers are attracted to Trend Micro’s fast synchronization of policies and reports designed to satisfy encryption readiness audits.

Cautions

- After a year in the market, Trend Micro has yet to establish competitive visibility, as evidenced in the lack of Gartner client inquiries and no feedback of it being a competitive threat from peers. EPP vendors that enter this market typically are quick to gain visibility among buyers based on their EPP history and the reputation of the acquired MDP. Trend Micro was unable to provide evidence of seat sales to assist Gartner to size or compare product penetration in the MDP market.

- Prospective buyers may be confused when searching for products to put on RFIs because the DataArmor and FileArmor products have been discontinued, but the transition is not prominently explained. The new suite of products is called Trend Micro Endpoint Encryption.

- Support for Mac OS X and Linux has been discontinued.
Competitive features involving DLP rule-driven encryption or file transfer blocking are not yet available and need further integration.

**Verdasys**

Verdasys is a longtime content-aware DLP player that has primarily focused on the intellectual property protection use case for DLP. Thus, it has developed encryption products that specifically address the protection and secure sharing of sensitive information within the context of a DLP framework. The resultant product qualifies for the MDP market. Verdasys encryption is now certified to FIPS 140-2 Overall Level 1. Platform support includes 32-bit Windows XP through 64-bit Windows 7, Windows Server and Linux. Windows 8 and OS X support are slated for the end of 2012.

**Strengths**

- Verdasys' understanding and integration of content-aware DLP and encryption are more mature than other vendors ranked in this Magic Quadrant, and include consumer mobile devices. Verdasys has developed a fully functional Digital Guardian family DLP agent for iPhone, iPad, Android and Windows Phone devices.
- Critical data and system files are encrypted, and all file access and movement activities can be monitored, controlled and audited in real time according to their enterprise DLP policy. Data (including files on removable media) encrypted by means of user-generated passwords can be recovered by the central agent if the user's password is lost.
- Because of the way the DLP and encryption features are implemented, Verdasys provides one of the strongest set of capabilities for the support of mobile sensitive data protection across multiple media form factors.

**Cautions**

- Verdasys is primarily known as a content-aware DLP provider and is not typically recognized as a competitor in this market. As a result, it typically does not appear in MDP-only shortlists. Buyers only consider Verdasys if they are already customers of Verdasys DLP, which limits its ability to communicate its MDP vision.
- MDP-related revenue and seat penetration are still relatively low but well within the criteria for inclusion.

**Wave Systems**

Wave Systems is the most experienced supplier of self-encrypting drive (SED) management, having pioneered the use of Seagate self-encrypting hard drives as the basis for managed FDE, and it was first to ship MDP products to support TCG encrypting drives from Hitachi and Samsung. In 2011, Wave Systems acquired Safend, which gave it ownership of products for file encryption and removable media protection. Wave Systems currently supports Windows XP through Windows 7. Windows 8 support is planned for 4Q12. Embedded system support includes Intel vPro, Seagate
encrypting drives, and all commercially available TCG encrypting drives and TPMs. Safend Encryptor and Safend Protector products can also support Mac OS X. The Safend acquisition provides ownership of FIPS 140-2 Overall Level 1 and CC certifications but only for file and removable media protection.

**Strengths**

- Safend’s historically successful niche track record is a helpful asset to gain buyer attention. Wave Systems can now break free from selling only pure-play Windows SED solutions, and will appeal to a wider set of buyers and end-user scenarios.
- A successful merger following a friendly, long-term OEM relationship has minimized the potential for disruptions in either company's operations.
- A dedicated TPM key management server helps companies back up TPM keys to an existing platform and migrate keys to new platforms for recovery or migration.
- Safend brings basic DLP capabilities to Wave Systems.

**Cautions**

- Wave Systems is integrating product lines; however, during this report’s evaluation period, they appeared as separate to the public eye. Prospects saw evidence of two companies, with no guidance about current or future product integration. Execution improvements are in doubt until the company begins to deliver on combined values.
- Wave Systems has leased a number of variants of its domain name, but buyers could still miss them when building an MDP RFI list. For example, "wavesystems.com" is owned by a company in a different security market and can cause dead-end searches.
- Gartner client feedback, a relatively low incidence of publication references or reviews, and lack of peer vendor reaction continue to signal a lowered standing in competitive execution.

**WinMagic**

WinMagic is a long-term, pure-play encryption provider with a comprehensive workstation product suite geared toward companies with high-security needs and strong authentication requirements. Platform support is provided for Windows 2000 through 64-bit Windows 7, Mac OS X, Linux, iOS and Android. Windows 8 support will be offered in timing with its release. Embedded system support includes Seagate encrypting drives, TCG encrypting drives, TPM, Intel AT and EFI. AES-NI is used to accelerate any type of SSD. On SEDs, WinMagic layers FIPS 140-2 encryption. WinMagic has certifications for FIPS 140-2 Overall Level 2 and CC EAL4.

**Strengths**

- WinMagic invests heavily in R&D. The company pioneered preboot authentication for encrypted hard drives, and supports local and remote preboot, OS-independent password reset, geotracking, theft deterrence and user deployment, as well as system and application software
update processes. WinMagic’s PBConnex can match many of the features and functions of Intel vPro and Anti-Theft (for example, in a CPU-independent, OS-independent configuration).

- A global reseller agreement with Lenovo, combined with hardware integration with Lenovo laptops, affords WinMagic an opportunity to raise future competitive visibility.
- Basic MDM and security support for iOS and Android is implemented directly in the MDP console.
- WinMagic can secure a multiuser system by means of a composite key that allows each user to have a unique startup PIN and SecureDoc file system associated to his or her unique Windows credentials. This has potential for BYOD use cases.
- As a specialized vendor, WinMagic is highly responsive to change requests. It has established a customer advisory board with long-standing clients to better analyze market feedback.

Cautions

- WinMagic sales overall are stable, but they are below the median and average for the market, and execution is indicative of the Visionaries quadrant.
- WinMagic’s primary buyers continue to be organizations with high security requirements. Although the company is making efforts to reach nontechnical buying centers, it sometimes misses the mainstream buyer with simple pragmatic concerns.
- The MDP market has a decreasing number of potentially interesting acquisition targets, and WinMagic has an attractive portfolio. Users should note that WinMagic has been considered for acquisition by many companies in related markets during the past year.

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.

Added

- No vendors were added to this edition of the report.

Dropped

- DigitalPersona was given a first ranking in last year’s report as a pure-play software as a service (SaaS) provider. The company has been removed from ranking this year because of a complete lack of competitive visibility according to the inclusion criteria during the study year, no response to this year’s survey and no encryption mention on its home page.
Safend was acquired by Wave Systems and is now ranked as part of Wave Systems.

Inclusion and Exclusion Criteria

Sixteen data protection vendors with MDP capabilities were notified of the annual survey. Twelve companies satisfied the inclusion/exclusion criteria and appear in the Magic Quadrant, according to the evaluation of these attributes:

- The vendor must have products that meet the market definition and were generally available in 2011 and in 1H12 for a sufficient length of time to attract market attention. The products must meet all aspects of the definition of products in the market, as set forth in this Magic Quadrant. The vendor must offer products for use on Windows-based PCs, because these 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.

- The vendor must be generally recognized as a participant in the market, as evidenced by Gartner client interest and inquiries, presence at tradeshows and conferences, and other forms of public and media mention that establish competitive presence. Our analysts must receive feedback from clients and case study reference organizations indicating that they are using the products. The vendor should appear regularly on Gartner clients’ shortlists for final selection and should 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.

- Companies that sell port controls and external/removable media protections as their only or main features, without meeting other core aspects of the MDP definition, did not qualify for inclusion in this Magic Quadrant.

- The vendor must own or license FIPS-140-2 certified encryption for the MDP product. Valid certifications may be acquired and, therefore, exist under several names. A vendor will be considered if its FIPS 140 application is processing during the study year.

- Seat sales in 2011 needed to total more than 125,000 seats, and 2011 revenue in the market must have been greater than $3 million. Exceptions may be granted if other inclusion factors merit consideration. These thresholds were continued from the prior report.

- The vendor must provide centrally managed access controls, lockouts, and key management/recovery and system recovery methods.

- The product must be commercially supported.

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

Vendors are asked to participate in an annual survey that is used to collect competitive and historical data within requested deadlines. If data is not provided, we estimate a vendor’s status from prior-year surveys, if available, and independent sources. Vendors that decline to report for several years in a row, and cannot otherwise be verified, may be excluded from or reduced in ranking consideration. Essential information that falls under this rule includes:

- Count of client companies under contract
- Count of seat sales (actual and estimated) over a three-year period
- Line of business (LOB) revenue, and other basic financial and organizational metrics

Vendors Considered but Not Included in the Magic Quadrant

- Absolute Software has never portrayed its encryption as a differentiated competitive product and is not generally identified as an encryption provider for the MDP market. The company will be reconsidered for next year’s report.

- Arkoon Network Security has provided evidence of credible market presence but does not meet the inclusion requirement for FIPS 140-2 certification. Although it is largely unknown for selling encryption products outside of France, the company has products that serve the needs of large companies, and may be a suitable choice for many buyers. Arkoon has received certification for CC EAL 3+.

- Hardware encryption subsystems, offered by vendors listed in the Market Overview section, are enabling technologies that may be exploited by MDP products, rather than complete solutions. Thus, they are not ranked in this Magic Quadrant.

- Open-source projects 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 when we see evidence of commercial support.

- SecurStar has been monitored for several years but has not yet met the inclusion requirement for FIPS 140 certification. Buyers should note that SecurStar’s website mentions the National Institute of Standards and Technology FIPS approved encryption and CC certification, but the company is not named on the portals of the relevant organizations.

- Companies that otherwise did not meet inclusion criteria and, in most cases, have not responded to requests for several years were not pursued and are no longer mentioned here.
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.

New products, new features and estimated sales in 1H12 were also considered in the final ranking. Unofficial road maps, pending contracts, future sales agreements, future promises for recent acquisitions, and vague strategies do not significantly contribute to a vendor ranking or to inclusion in this Magic Quadrant; however, vendors that have official and public road maps, and make consistent progress, are recognized.

Execution weightings are considered standard because, within the research review, the relative merit of each ranking factor can be adequately expressed for the general case without additional adjustments. Weightings are contextual. Readers who conduct their own RFIs may choose to change weightings to suit the needs of their business and their industry:

- **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 are considered.

- **Sales Execution/Pricing** compares the strength of a vendor’s sales and distribution operations, 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 will respond to sales techniques led by case studies and ROI projections.

- **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 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.
One of the interesting interpretive elements of the survey is an execution question in which vendors are asked to name three peers that constitute their greatest competitive threat. The result of this survey question is a good barometer for understanding the potential of vendors to maintain high performance in this market.

Table 1. Ability to Execute Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product/Service</td>
<td>Standard</td>
</tr>
<tr>
<td>Overall Viability (Business Unit, Financial, Strategy, Organization)</td>
<td>Standard</td>
</tr>
<tr>
<td>Sales Execution/Pricing</td>
<td>Standard</td>
</tr>
<tr>
<td>Market Responsiveness and Track Record</td>
<td>No Rating</td>
</tr>
<tr>
<td>Marketing Execution</td>
<td>Standard</td>
</tr>
<tr>
<td>Customer Experience</td>
<td>Standard</td>
</tr>
<tr>
<td>Operations</td>
<td>No Rating</td>
</tr>
</tbody>
</table>

Source: Gartner (September 2012)

Completeness of Vision

Vision is ranked according to a vendor’s ability to show a broad commitment to technology developments in anticipation of user wants and needs that turn out to be on target with the market.

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.

Vision weightings are considered standard because, within the research review, the relative merit of each ranking factor can be adequately expressed for the general case without additional adjustments. Weightings are contextual. Readers who conduct their own RFIs may choose to change weightings to suit the needs of their business and their industry:

- **Market Understanding** and **Marketing Strategy** are ranked together as **Marketing Strategy**, and are assessed through direct observation of the degree to which a vendor’s products, road maps and missions anticipate leading-edge thinking about buyers’ wants and needs. Gartner makes this assessment by several means, including interactions 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. A
vendor cannot merely state an aggressive future goal. It must put plans in place, show that it is following the plans, and modify plans as market directions change. Also considered are the vendor’s partnerships with other vendors in related endpoint security markets, including antivirus, anti-spyware, configuration management, authentication, device identification, VPNs, 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.

- **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. However, this Magic Quadrant doesn’t consider vertical markets as a distinctive ranking factor, so this category is irrelevant and not rated.

- **Innovation** takes into consideration the degree to which a vendor invests in core requirements for the successful use of its 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, detailed examination and ranking of this category are irrelevant. In 2010, North America was estimated to account for more than 63% of MDP revenue potential (on average) and, for many years, success in the North American geography has been the primary indicator of viability. Buyers in other geographies tend to react to vendors based on their competitiveness in North America and, to a lesser extent, in Europe.
### Table 2. Completeness of Vision Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Understanding</td>
<td>No Rating</td>
</tr>
<tr>
<td>Marketing Strategy</td>
<td>Standard</td>
</tr>
<tr>
<td>Sales Strategy</td>
<td>No Rating</td>
</tr>
<tr>
<td>Offering (Product) Strategy</td>
<td>Standard</td>
</tr>
<tr>
<td>Business Model</td>
<td>Standard</td>
</tr>
<tr>
<td>Vertical/Industry Strategy</td>
<td>No Rating</td>
</tr>
<tr>
<td>Innovation</td>
<td>Standard</td>
</tr>
<tr>
<td>Geographic Strategy</td>
<td>No Rating</td>
</tr>
</tbody>
</table>

Source: Gartner (September 2012)

### Quadrant Descriptions

#### 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 are frequently found on RFP shortlists.

#### Challengers

Challengers have competitive visibility, market share, and financial and channel strengths that are better-developed than Niche Players, but not as broad as Leaders or Visionaries. They also have greater success in sales and mind share than similar Niche Players. Challengers offer all the core features of MDP, but typically their vision, road maps or product delivery are narrower than the Leaders. Challengers may have difficulty communicating or delivering their vision in a competitive way, but they can be very disruptive to the sales of other vendors, particularly Leaders. 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. The Magic Quadrant for MDP historically reports little or no activity in this quadrant. In general, companies that execute strongly become Leaders.
Visionaries

Visionaries make investments in broad functionality and platform support, but their competitive clout, visibility and market share don’t reach the level of Leaders. Visionaries make planning choices that will meet future buyer demands, and they assume some risk in the bargain, because ROI timing may not be certain. Companies that pursue Visionary activities will not be fully credited if their actions are not generating noticeable competitive clout and are not influencing other vendors. The difference between Visionaries and Niche Players amounts to the risks that the company takes in terms of strategic R&D and the ability to realize competitive clout from those risks.

Niche Players

Niche Players offer products that suit many enterprises’ needs and often are the best choice to get a stable product, combined with more-personalized service. A Niche Player 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. 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 in the market (which would be expected of a Visionary). Niche Players are candidates for acquisitions.

Context

MDP systems and procedures are needed to protect business data privacy, meet regulatory and contractual requirements, and comply with audits. This Magic Quadrant is a market snapshot that ranks vendors according to competitive buying criteria. Vendors in any sector of the Magic Quadrant, as well as those not ranked on the Magic Quadrant, may be appropriate for your enterprise’s needs and budget. Every company must include MDP in its IT operations plan.

Market Overview

MDP is an established market with two primary purposes — first and foremost, to safeguard user device data by means of encryption and authentication; and second, to provide evidence that the protection is working. Most companies, even if not in sensitive or regulated industries, recognize that encrypting business data is a best practice. Common motivations for protecting data are to comply with government or industry regulations, maintain privacy, and shield intellectual property. Legislation across the world mandates increasingly tough penalties, as well as requirements for public disclosure in the event of a real or suspected mishandling of personally identifiable information. Even if information is not misused, the public relations costs to quell negative public reaction are expensive. Gartner believes that the costs of a data breach are always higher than the cost to invest in preventive measures, such as MDP (see “Pay for Mobile Data Encryption Upfront, or Pay More Later”).
Press notifications of breach disclosures, mitigations and fines drive interest and inquiry into deployment of MDP, and there is evidence that a significant number of systems are still unprotected. For example, a 4Q11 online survey of 150 satisfied enterprise users conducted for the EPP Magic Quadrant indicated that 35% still had not installed encryption protection. Most companies that invest in MDP conduct only partial installations for notebook/laptop computers, so there is still considerable room to upgrade and upsell to desktop and server platforms, including PCs, Macs and Linux-based systems, and to tie in with MDM. Furthermore, many data exposures happen on desktop and server platforms. Gartner recommends that all companies make efforts to broadly install encryption across their endpoint platforms.

Products in this market typically support several workstation platforms. However, public focus and most sales dwell on notebook (laptop) computers running versions of the Windows OS, because they are the most common business workstation platforms to be cited in stories of loss, theft and penalties. They also represent the most predictable sources of revenue.

The influence of EPP vendors that have acquired MDP products is significant. EPP product suites are the most obvious of several places for encryption to add value for workstation buyers, because EPP vendors already aggregate the other most common security needs, including enterprise antivirus, anti-spyware, personal firewall and desktop host intrusion prevention systems. For most organizations, selecting an MDP system from their incumbent EPP vendors will meet their requirements.

LOB revenue is useful to gauge a company’s health and ability to execute, and many companies ranked in this Magic Quadrant cannot otherwise separate the MDP revenue from the LOB containing MDP. According to information derived from the 2012 Magic Quadrant survey results, 2011 worldwide revenue in the LOB containing MDP was estimated at $683 million — down from about $715 million in the previous report. Decreases reflect discounted pricing from EPP vendors, a merger, some uptake of Microsoft BitLocker and increasing challenges for stand-alone vendors to differentiate their offerings.

At the same time that estimated revenue has reduced, seats sold in the market have increased. Based on the 2012 Magic Quadrant survey results, seats sold for 2011 (a combination of reported and estimated data) increased to about 43 million, compared to 32 million seats for 2010, 23 million seats for 2009 and 28 million seats for 2008. Three-year cumulative seats sold (2009 plus 2010 plus 2011) are estimated at 100 million.

MDP earns a caution assessment for growth in 2012 through 2013. The fact that a Gartner survey of qualified companies that otherwise understand the value of EPP uncovered 35% without encryption can also mean that the effort to sell encryption to “stragglers” is getting more difficult. Half of the clients who called for EPP advice in 2010 intended to include MDP in their EPP buying decision. In 4Q11, the same Gartner survey indicated that only 20% of companies would choose an EPP vendor because of a compelling MDP product.

All vendors and all products tracked in this Magic Quadrant offer similar basic functions, and use comparable encryption algorithms and management functions. Differences in the Ability to Execute are based largely on financial and sales performance, but are strongly influenced by client feedback,
and anecdotal research into matters of satisfaction and usability. Differences in Vision are scaled according to the breadth of the platform and the ability of a company to anticipate hot buying issues, as evidenced by their R&D investments.

Opportunities for MDP innovation will be limited in the next several years. At present, the competitive "final frontier" for workstation MDP is mainly limited to incremental support improvements for SEDs, removable media and Mac OS X support. Attempts to generate growth from MDP offered as a cloud service continue to stall. Gartner also sees little current overlap between MDP and a related market for MDM aimed at smartphones and tablets. MDM tools can manage and supplement encryption, and are usually treated as a separate buying decision, even when it involves a vendor that also sells MDP and EPP.

**Features, Technologies and Client Concerns for 2012 and 2013**

Gartner clients know that data leakage can cost them money and their reputations, 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:

- **Performance:** New workstations with multicore processors and ample memory have erased most legacy performance concerns. Reference clients still report variable quality experiences that can be traced to implementation errors. Gartner advises trial tests before production rollouts, and backups before installation on devices in use.

- **Entry price:** In small quantities (fewer than 500 seats), list seat pricing, prior to negotiation, for an MDP suite ranges from $125 down to $30 per seat. Additional costs can include several consulting days for installation and training, support/maintenance (typically 20% or more of contract value), and, in smaller contracts, there may be a separate fee for the management console. For financial reasons, smaller MDP companies may be unable to deeply discount their products, but are still attractive for personalized service and specialized use cases. EPP vendors that have entered the MDP market are better targets for aggressive pricing negotiations, even though EPP and MDP are not significantly integrated in most cases.

- **Encryption offered as a managed cloud service (SaaS):** Gartner believes that MDP offered as a trusted service makes sense and can reduce barriers to entry, particularly for smaller companies. However, MDP vendors have historically been unsuccessful at growing SaaS offerings into significant revenue, and the trend continues. SaaS continues to represent less than 1% of the total MDP market value of vendors tracked in this Magic Quadrant. MDP as SaaS must be seamlessly bundled with EPP to succeed, because EPP has been accepted as a SaaS model for many years.

- **Government security certifications:** FIPS 140-2 and CC are generally recognized by all buyers as signs of competence and commitment by an MDP vendor. FIPS 140-2 is the current standard for robust cryptographic engines in the MDP market, and is a requirement for federal government purchases. Gartner recommends FIPS 140-2-certified encryption for all purchases. CC certification is a true international validation that documents product specifications in a standard format.
- **Non-Microsoft- Windows workstations:** Gartner sees increasing interest in supporting Apple Mac OS X workstations, and scant mention of Linux and Unix platforms. Product features are not always complete on secondary platforms, and buyers are advised to perform thorough evaluations, as well as request road map presentations, during the RFP phase.

- **Multiuser scenarios:** Enterprise MDP tools designed for FDE do not efficiently serve the needs to protect information on personal or multitenant/multiuser devices. Protection for personal workstations seems better suited to virtual machines (which can run MDP within), MDP tools based on file encryption (which defend Windows at startup and natively support roaming profiles), quarantined browser sessions (supported by secure browsers and Secure Sockets Layer [SSL] VPNs), and self-encrypting applications specially built and selected for personal use cases.

- **BYOD:** For reasons similar to multiuser scenarios, enterprise MDP tools designed for FDE and a single user are too disruptive to install on a user’s personal workstation. File-based encryption products that allow Windows to start — and subsequently can manage several secure and separated user accounts — may be a better choice. However, virtual machines, quarantined browser sessions (supported by secure browsers and SSL VPNs), and self-encrypting applications specially built and selected to isolate business operations on unmanaged workstations can be better alternatives.

- **Smartphones and tablets:** MDP vendors are moving into the small device marketplace, primarily through MDM. Several vendors that are offering MDP for consumer mobile devices have not garnered competitive market share by this means, because clients respond instead to the MDM market definition and range of functions.

- **Hardware subsystems:** Buyers have several choices among hardware systems to improve the performance of MDP investments. The most significant has proved to be SEDs based on TCG’s open-industry standard, usually referred to as Opal. SEDs are valued by users who try them; however, availability was limited through 2011, and SEDs may continue to be scarce in 2012, hampering the attempts of many companies to standardize on them. Buyers should select MDP tools that can still provide all the necessary functions and compliance certifications in software to compensate for platforms that lack a particular hardware component. Note that a new family of SEDs based on Opal Security Subsystem Class 2.10 and UEFI 2.3.1 will be supported by Windows 8.

- **Key management, storage and destruction methods:** Key issues are frequently on buyers’ minds because of valid concerns regarding the misuse of user/system key/access credentials resulting from inside attacks, loss, theft and hacking. Poorly managed key methods can result in loss of keys and, therefore, loss of access to critical data. Lax administration controls may allow key access to unauthorized people. Poorly architected or weakly configured encryption products may be vulnerable to brute force or dictionary key recovery on the client device. A well-managed and crafted key system not only avoids these problems, but also provides disposal protection tantamount to drive wiping, and is essential to defend against data breaches on lost systems. Buyers are advised to perform thorough evaluations on all applicable use cases.
Recommended Reading

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

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Hype Cycle for Data and Collaboration Security, 2012"

"Magic Quadrant for Mobile Device Management Software"

"Quarterly Statistics: Personal Computers, All Countries Forecast Database, 2Q12 Update"

"Pay for Mobile Data Encryption Upfront, or Pay More Later"

"Protecting Sensitive Data on Decommissioned SSDs and HDDs"

"Best Practices for Data Destruction"

"Implementation Advice for Mobile Data Protection"

"How to Avoid Mobile Data Protection Failures"

Evidence

"Microsoft BitLocker Administration and Monitoring (MBAM) Documentation Resources Download Page."

Microsoft's "Encrypted Hard Drive Device Guide."

Common Criteria portal.

NIST's "FIPS 140-1 and FIPS 140-2 Vendor List."

McAfee announcement about FIPS certification and AES-NI.

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 and skills, 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 presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

Market Responsiveness 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 and SLAs.

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 products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor’s approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature 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.
Regional Headquarters

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

**Japan Headquarters**  
Gartner Japan Ltd.  
Atago Green Hills MORI Tower 5F  
2-5-1 Atago, Minato-ku  
Tokyo 105-6205  
JAPAN  
+ 81 3 6430 1800

**European Headquarters**  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

**Latin America Headquarters**  
Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509

**Asia/Pacific Headquarters**  
Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

© 2012 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner’s research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity” on its website, [http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp](http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp).