


Magic Quadrant for Mobile Data Protection

Published: 8 September 2014

Analyst(s): John Girard

Mobile data protection solutions defend access to secure data on storage systems in notebooks, removable media, desktops, servers and, in a few cases, cloud storage environments. Buyers seek data protection policy enforcements across multiple platforms, minimal support costs and proof of protection.

Additional Perspectives

 Company Size: [Small & Midsize \(<1000 Employees\)](#)

Strategic Planning Assumption

Based on a small exposure scenario, the cost to mitigate a simple data breach will cost more than 70 times the original price to implement encryption.

Market Definition/Description

Gartner defines mobile data protection (MDP) products and services as software security methods that enforce confidentiality policies by encrypting data, and then defending access to that encrypted data on the primary and secondary storage systems of end-user workstations. These storage systems include the primary boot drive of a workstation and removable devices used for portability. Storage technologies affected by MDP include magnetic hard-disk drives (HDDs), solid-state drives (SSDs), self-encrypting drives (SEDs), flash drives and optical media. Some vendors also have protection capabilities for network storage, and a few also support cloud-based storage environments as an extension to the desktop.

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

MDP products qualified for inclusion in this report must have both local/device-level agents and central management. A central console 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 manages encryption and access controls on the target device. Data copied to removable media may be encrypted and accompanied by a

portable software security agent. Agents can respond to central server directives, or can take local actions to lock, wipe and recover a device that falls out of compliance. Ranked vendors must have U.S. Federal Information Processing Standard (FIPS) 140-2 certification in their owned or licensed code for at least their main encryption system as a proof of strong commitment to data protection. Participation is also expected in multinational guidelines such as Common Criteria (CC).

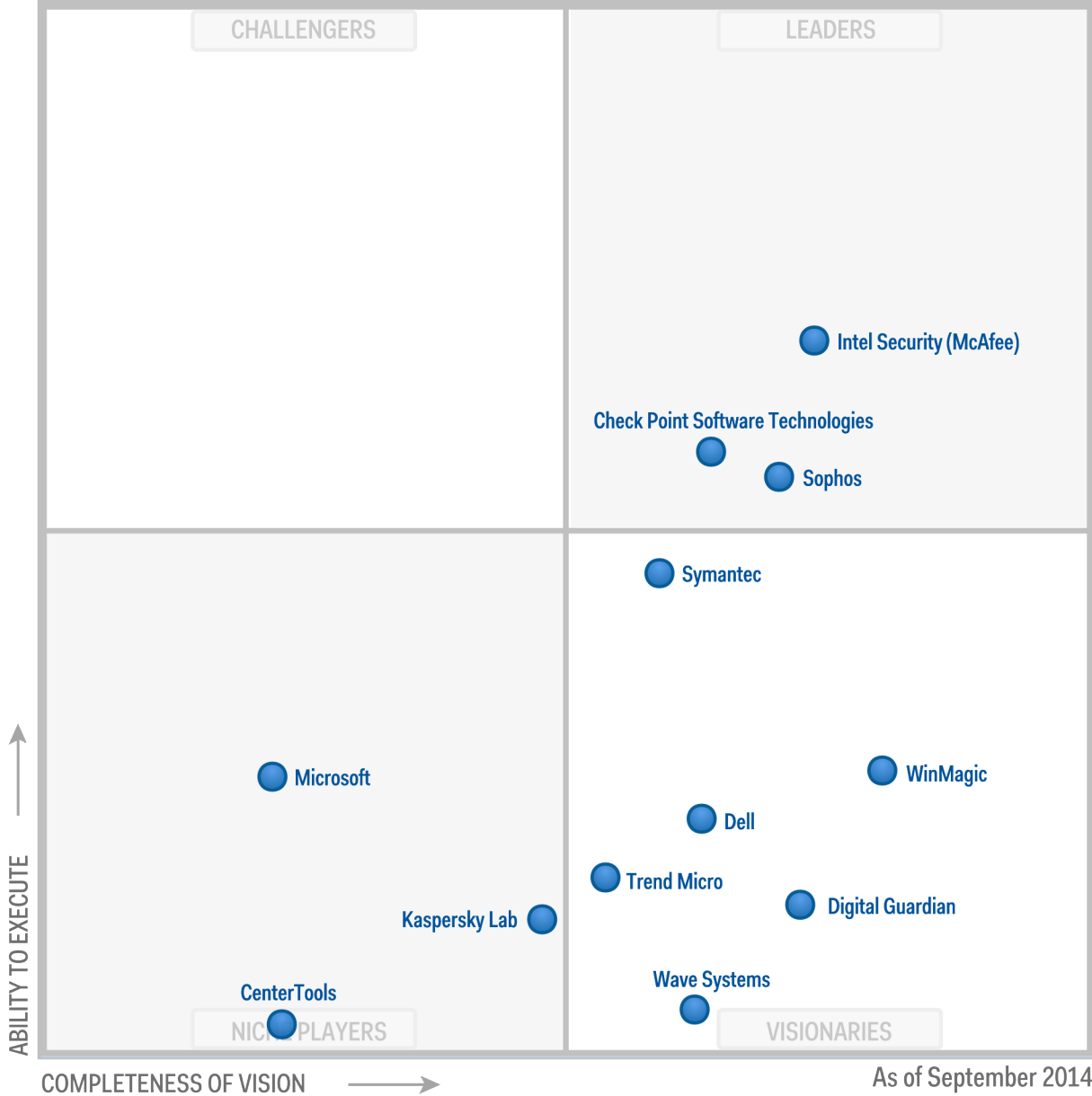
MDP functions integrate with the OS and underlying firmware services of their host platforms, so they can control storage input/output and insert themselves in the primary steps of user authentication. With few exceptions, MDP vendors are capable of providing all encryption/decryption processes as software 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, and to native capabilities in the OS. However, MDP cannot simply be replaced or made obsolete by the presence of embedded encryption engines. A central MDP management framework will always be the focal point for encryption policy management, key access and storage, and backup, system recovery and audit reports.

MDP-managed encryption may be invoked at the level of individual files or at the folder, partition or full drive/volume, depending on the use case. The latter method, which is the most common, is typically called full-disk encryption (FDE). Authentication must occur to gain access to data. This is done by a login event and perhaps other stronger secondary authentication, which may range from a simple PIN to a complex password, token or smart card, and may also use biometrics, geolocation, LAN identity, and so on.

The majority of MDP revenue is generated from sales to support computers based on the Windows OS, but buyers frequently request Mac OS X support. Therefore, additional consideration was given to vendors that cross multiple platforms and OSs. Configuration management support for smartphones and tablets running nonworkstation OSs is satisfied by a different market called enterprise mobility management (EMM — formerly mobile device management [MDM]). Several vendors in this report have EMM/MDM products and services. EMM is generally not integrated with MDP, nor does it generally offer FDE or file encryption. Buyers indicate to Gartner that they treat the purchases separately.

Magic Quadrant

Figure 1. Magic Quadrant for Mobile Data Protection



Source: Gartner (September 2014)

Vendor Strengths and Cautions

CenterTools

CenterTools has offered DriveLock encryption in European markets since 2003. Platform support is provided for Windows 7 and 8 except RT, and password-protected file viewers are offered for Android, and iOS. CenterTools owns the SafeNet cryptographic module for FDE, which is FIPS 140-2 certified to Level 2 in software and uses FIPS-certified OpenSSL for file and folder encryption. CenterTools does more than 84% of its current business in Europe, making it a geographical niche choice for midsize enterprise European buyers. Additional support is provided for Intel AES-NI.

Strengths

- European mobile security buyers are more likely to consider non-U.S. vendors like CenterTools as a result of concerns over intelligence gathering activities.
- DriveLock File Protection supports on-device managed encrypted file sharing for cloud services via Windows, OS X, iOS and Android devices, and is included in the standard bundle.
- Screen touch keyboard is supported for preboot authentication on Windows tablets. Nonbooting tablets may be recovered from the touchscreen using a recovery agent on a flash drive.

Cautions

- DriveLock 7.3 was unable to automatically lock/wipe a system that has failed to sync with a management server after a threshold has passed — for example, a system out of contact for defined period, such as 14 days.
- Neither UEFI nor self-encrypting drives are supported at this time. No tests are currently included to detect or react to tampering within a protected device.
- System management can only be performed through MMC; no Web console is provided.

Check Point Software Technologies

Check Point Software Technologies has offered MDP since 2007. Platform support is provided for Windows 7 and 8 except RT, and for Mac OS X and major Linux distributions such as Red Hat distros including Fedora and Red Hat Enterprise Linux (RHEL), and Mandriva and SUSE. A policy-compatible encrypted container with VPN is available for consumer smartphones and tablets. Check Point is FIPS 140-2 certified to Level 1 in software, and was awarded CC EAL4. Additional support is provided for UEFI, Opal SEDs and TPM.

Strengths

- Check Point's primary headquarters is located in Israel. Non-U.S. businesses may be at an advantage in the current cautionary buying climate that has otherwise impacted many U.S.- and China-based companies attempting to sell abroad.

- Check Point's help desk system can be integrated into any third-party support system, such as Hitachi ID Systems.
- Alternate cryptography and local partner assistance are available in foreign countries with prohibitive crypto regulations, such as China and Russia.
- Check Point provides secure, audited document access for all major OSs and platforms, and can integrate with rights management in Microsoft Office, Adobe and notepad applications.

Cautions

- Check Point's pricing model is typically more expensive than comparable MDP offerings in the market.
- Check Point is not competitively visible in the MDP market, whether through Gartner client interaction or from third-party sources. It is mainly encountered in companies that have existing infrastructure investments from the vendor.
- Check Point has not added native support for BitLocker or FileVault 2.
- Workstation boot behavior and media access controls can be affected by location — that is, "unlock on LAN" — however, removable media with portable encryption cannot be made location-aware.

Dell

Dell Data Protection is built on technologies acquired from Credant in 2013. Platform support is provided for Windows 7 and 8 except RT, and Mac OS X, and compatible agents have been released for iOS and Android devices. Dell Enterprise Mobility Management (EMM) is provided in a separate product with a road map to integrate cross-platform policies for small and large devices, as well as "BYO." Dell is certified to FIPS 140-2 Level 2 in software and Level 3 in Dell hardware, and was awarded CC EAL3. Additional support is provided for BitLocker, FileVault 2, Seagate Technology SEDs and Opal SEDs, TPM and UEFI.

Strengths

- Dell's high levels of FIPS certification and standard FIPS operational modes (FIPS 140-2 cannot be deselected) demonstrate an earnest commitment to strong data protection. Software product versions are available for non-Dell platforms.
- Dell offers comprehensive protection without full-disk encryption or preboot authentication that works with conventional wake-on-LAN, system diagnostic and imaging tools, multiuser workstations, and roaming profiles. Full-disk encryption and SED configurations are also available. Dell works with customers to ensure access to SEDs.
- Dell has deeply discounted its management support fees for BitLocker.

Cautions

- Non-Dell buyers don't generally recognize Dell Data Protection as a choice for use on other platforms, even though it is available for non-Dell systems.
- Dell has not committed to a data loss prevention (DLP) road map to bring contextual rules to the decision to encrypt files.
- Product versions that were generally available during the evaluation period did not keep logs for data written to external media.

Digital Guardian

Digital Guardian, formerly Verdasys, is a longtime content-aware player with premium tools focused on encrypting and protecting intellectual property in a DLP framework. Platform support includes Windows 7 and 8 except RT, and for Mac OS X and Linux distributions including Red Hat, CentOS, Oracle, SUSE and Ubuntu. A fully compatible Digital Guardian app is offered for iOS. Verdasys is certified to FIPS 140-2 Level 1 and was awarded CC EAL2+.

Strengths

- Digital Guardian's understanding and integration of content-aware DLP is extensive and mature, and represents the required practices for data protection in next-generation mobile security systems.
- Because of the way the DLP and encryption features are implemented, Digital Guardian provides one of the strongest sets of capabilities for the support of mobile-sensitive data protection across multiple media form factors, including popular smartphones and tablets.
- Digital Guardian is the only vendor in the study that has significant revenue share from cloud-hosted services.

Cautions

- Digital Guardian typically does not appear in MDP-only shortlists, and MDP is not a major line of business. Buyers consider Digital Guardian if they are already customers of the company's DLP, which limits its ability to communicate its MDP vision and minimizes direct competition.
- Digital Guardian does not have integrated support for many of the advanced and/or embedded encryption technologies, such as SEDs, BitLocker, FileVault 2, Intel AES-NI, TPM, and so on.
- Digital Guardian is adjusting its internal priorities to address a broader insider/outsider advance threat defense use case. This puts the company into more direct competition with established EPP and MDP vendors where Verdasys was relatively unknown, and faces a set of buyers that are not accustomed to investing in companies originating in DLP markets.

Intel Security (McAfee)

The integration by McAfee, part of Intel Security, of SafeBoot MDP into its Complete Data Protection Suites and McAfee ePolicy Orchestrator (ePO) management architecture is among the most successful by an endpoint protection platform (EPP) vendor. Platform support is provided for Windows 7 and 8 except RT, and for Mac OS X. Support for consumer smartphones and tablets is offered in a separate product, McAfee Enterprise Mobility Management, which reports into a single integrated console. McAfee is certified to FIPS 140-2 Level 1 in software and was awarded CC EAL4. Additional support is provided for BitLocker, FileVault 2, Intel AES-NI, UEFI and Opal SEDs.

Strengths

- Gartner client inquiries strongly recognize Intel Security's presence in this market, and their intersection with the endpoint protection market. Seat penetrations for the company's MDP and line of business (LOB) revenue are the highest in the survey. It tied with Microsoft as the greatest competitive threat as rated by its peer group in this year's MDP survey.
- The Endpoint Encryption Go (EEGO) utility performs a thorough analysis on systems to determine which encryption technologies can be used, and will predict and prevent installation failures as well as future problems.
- Standard maintenance support, automated Windows platform migration and online training are included at no extra charge, and the company will negotiate attractive pricing in order to win deals among incumbent customers.

Cautions

- The full-volume secure vault for USB flash drives presents an Explorer-like interface but doesn't fully support Windows drag-and-drop file operations. Users may be confused about how to open and save files.
- Software encryption for 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 for Mac OS X users.
- TPM-protected drives can be migrated to new systems using an offline user challenge/response, which does not require the help desk to be aware or for approval to be required.
- Intel Security does not provide a method for escrow-quality data protection.

Kaspersky Lab

Kaspersky Lab is a Russian-based endpoint protection vendor. Kaspersky's encryption solution became available for sale in 2013, too late to be considered for last year's edition of the Magic Quadrant. Platform support is provided for Windows 7 and 8 except RT. Kaspersky's endpoint protection suite, removable media protection, as well as basic EMM for smartphones and tablets, are integrated in a single offering. Kaspersky uses third-party FIPS 140-2 certified cryptography at this time. Additional support is provided for AES-NI.

Strengths

- Kaspersky has a strong general reputation for rapid reaction and comprehensive mitigations to security events.
- The company has an unusually balanced sales share ranging from very small to very large companies, demonstrating the agility to support a wide range of end-user scenarios, and contributing to its viability as an end-user investment.
- European mobile security buyers, particularly in the eastern European countries, are more likely to consider non-U.S. vendors like Kaspersky as a result of concerns about intelligence gathering activities.

Cautions

- Neither UEFI nor Windows tablets were supported by product versions available during the evaluation period.
- Secure platform lockup/data destruction functions are only available for smartphones.
- Secure portable media viewing is limited to Windows platforms only.

Microsoft

Microsoft meets the inclusion criteria if, and only if, its solution is considered to be a combination of the embedded BitLocker engine and its central management system known as Microsoft BitLocker Administration and Monitoring (MBAM), which is available through Microsoft Desktop Optimization Pack (MDOP). The combination supports workstations operating Windows 7 Enterprise and Ultimate editions, Windows 8 Pro and Enterprise editions, and any version of Windows 8.1 or higher. BitLocker is certified to FIPS 140-2 Level 1, and MBAM gained FIPS mode support near the end of the evaluation period. Additional support includes TPM, UEFI and Opal SEDs.

Strengths

- BitLocker is included with the OS. Companies already investing in MDOP have access to MBAM.
- Microsoft tied for first place with Intel Security among peers ranking each other for competitive threat.
- MBAM can detect unprotected workstations on the LAN and force activation of encryption.

Cautions

- Companies that needed to protect Macs, Linux and nonenterprise Windows 7 editions found it necessary to maintain additional MDP products and services. Other MDP vendors in this market have been putting BitLocker under FIPS-140-2 management, and integrating it into cross-platform solutions at price levels comparable to or less than the estimated value of MBAM. Many users consider BitLocker on the basis that it's free and fail to deploy it with enterprise

management capability (for example, MBAM), resulting in configurations that don't meet Gartner's recommendations for MDP.

- On conventional workstations, the startup PIN is required to implement preboot protection.

Sophos

Sophos SafeGuard Encryption, built from Utimaco Safeware, interoperates with the company's Endpoint Security Antivirus protection suite. Platform support is provided for Windows 7 and 8 except RT, and for Mac OS X. Sophos Mobile Control and Sophos Mobile Encryption are separate EMM products supporting consumer smartphones and tablets. Sophos is certified to FIPS 140-2 Level 1 on PCs, and was awarded CC EAL3+ and CC EAL4. Additional support is provided for FileVault 2, BitLocker, TPM, Opal SEDs, Intel AES-NI, vPro and UEFI.

Strengths

- Sophos' primary headquarters is in the U.K. A European span of control plus European government purchase approvals have been helpful for Sophos in the cautionary buying climate concerning intelligence gathering activities that has otherwise impacted many U.S.-based companies attempting to sell abroad.
- Sophos' steady progress and growth in MDP improves its credibility in the market, and makes continued focus and investment in broader areas of data protection, including its Data Protection Everywhere, a good bet for enterprise buyers.
- FIPS-level support for BitLocker is available in the standard product, or stand-alone for a perpetual price point that undercuts the estimated investment value for MBAM.

Cautions

- Sophos does not provide policy adjustments for geographic location, network identity or off-network conditions.
- Although Sophos embeds DLP features, there is no current integration with third-party rights management systems.
- Sophos DLP cannot invoke encryption or block writing based on keywords or other content decisions. An API is available for users to write their own filters.

Symantec

Symantec acquired PGP and GuardianEdge in 1H10 and has labored since then to put them together. PGP Whole Disk Encryption (PGP WDE) has been rebranded as Symantec Drive Encryption (SDE). Platform support includes Windows 7 and 8 except RT, Mac OS X and Linux distributions including Ubuntu, RHEL, CentOS, SUSE and SUSE Linux Enterprise Server (SLES). The optional Symantec Mobile Encryption for iOS facilitates the sending and receiving of PGP-encrypted email on iPhones and iPads. Symantec Mobile Management is a separate EMM product

supporting consumer smartphones and tablets. Additional support is provided for Intel AES-NI and Opal SEDs. Symantec is certified to FIPS 140-2 Level 1 in software, and was awarded CC EAL2 and CC EAL4+.

Strengths

- Symantec has an extensive global network for sales, service and support, and ranked third in a survey among its peers for competitive MDP threat.
- Policy-compatible encryption can be enforced on files sent to email using Symantec DLP, and external shared storage, such as cloud systems, using Symantec File Share Encryption, all for additional fees.
- Symantec's presence in multiple adjacent data protection markets including DLP, EPP, EMM, identity and access management (IAM) and secure email gateway (SEG) are attractive to MDP buyers seeking a single vendor relationship.

Cautions

- Symantec did not complete integration of its MDP products during the evaluation period and has offered license exchange plans that customers find confusing.
- Symantec has not released native encryption support for Opal SEDs, BitLocker or FileVault 2 during 2014, and has announced end of life for TPM support.
- Symantec does not offer a method to change boot behavior based on detecting connections to trusted networks, geolocations, and so on.

Trend Micro

Trend Micro offers MDP based on technologies acquired from Mobile Armor in 2011. Platform support is provided for Windows 7 and 8 except RT. EMM for consumer smartphones and tablets is available in separate products, but manageable under a common console. Trend Micro is certified to FIPS 140-2 Level 2 and was awarded CC EAL4+. Additional support is provided for BitLocker, FileVault 2, Seagate and Opal SEDs, TPM and Intel AES-NI.

Strengths

- Trend Micro's main headquarters is in Japan and its largest companywide revenue come from Asia/Pacific, with European revenue second. This is a tactical advantage in a period where U.S. security companies are facing increased challenges to sell abroad due to concerns about intelligence gathering.
- Removable media access policy can be set to require remote authentication (to a company server). It can also set a policy to require remote authentication after a number of failed offline logins, or after a specific date.
- MDP is licensed per user, and for one price, it can be installed on all of a user's devices.

- Trend Micro installs and operates in FIPS compliant modes by default.

Cautions

- Trend Micro does not typically appear in shortlist discussions for MDP, and mainly gets business by selling to existing customers. Market presence is on a par with small players.
- In North America, Trend Micro relies completely on resellers.
- Trend Micro offers optional managed secure sync and file share tools but cannot detect and force encryption if the user writes files to an unauthorized network or cloud storage system.
- Product versions generally available during the evaluation period only supported UEFI-dependent devices through BitLocker.

Wave Systems

Wave Systems pioneered the use of SEDs. The 2011 Safend acquisition brought DLP, file protection and removable media encryption in-house. Platform support includes Windows 7 and 8 except RT, and Mac OS X. Through the Safend acquisition, Wave is certified to FIPS 140-2 Level 1 and has CC certifications for file and removable media protection. Additional support is provided for BitLocker, FileVault 2, Seagate and Opal SEDs, TPM and UEFI.

Strengths

- The baseline platform contains all major features, including DLP policies. The DLP filter is content-aware and also can recognize and catalog external cloud storage systems on the fly.
- The Wave ERAS management server automatically backs up and securely stores TPM keys for recovery or migration. Help desk recovery information is stored in Microsoft Application Directory but is strongly defended. Trusted drives can be easily moved and reauthorized remotely.
- Wave can perform detailed geolocation detection — beyond just verifying a LAN, which can be used to make granular changes to system boot behavior and access controls.
- Wave can detect and activate workstation encryption, including BitLocker-enabled devices, inside and outside of the firewall.

Cautions

- Wave Systems has made board-level changes aimed at prioritizing growth opportunities. However, given a recent history of operating at a loss, buyers should monitor company performance.
- Wave takes a strict view of external media that does not allow for mixed encrypted and unencrypted files — for example, on USB drives. However, many companies indicate a preference for flexibility, especially for non-company-owned media.

- 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 has sold complete workstation encryption solutions since 1997. SecureDoc is geared toward companies with high-security needs and strong authentication requirements. Platform support is provided for Windows 7 and 8 except RT, and all major Linux distributions in SED configurations. Fully managed and compatible SecureDoc agents have also been released for consumer smartphones and tablets. Additional support includes SEDs, TPM, Intel AES-NI, BitLocker, FileVault 2 and UEFI. WinMagic is certified to FIPS 140-2 Level 1 and was awarded CC EAL4.

Strengths

- WinMagic is an increasingly strong candidate for APAC buyers, particularly in China, where WinMagic has been awarded purchase approvals and has Lenovo as a local sponsoring partner.
- WinMagic offers a single integrated console view of all encrypted systems, policies and encryption engines, including smartphones and tablets.
- Contract examples reviewed by Gartner indicate that the company will negotiate attractive pricing in order to win deals.

Cautions

- Clients have expressed concern with the size of the company and its seemingly narrow focus on very high security buyers, but should be reassured by WinMagic's long time in the industry.
- WinMagic does not distinguish between data written to a network file system, a file sync service and the normal file system, nor does it provide blocking based on a specific use case or context.
- The moving of drives protected by TPMs requires a manual intervention to convert to a non-TPM-protected keyfile.

Vendors Added and 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

- Kaspersky Lab released an MDP product in 1Q13, and satisfied the criteria for this year's report.

Dropped

- Novell's NetWare Enterprise Print Services (NEPS) has not been visible in client inquiry demands or in encryption market research in general. Competitive revenue and seat data for several years were also not available. Gartner will monitor Novell's progress and reassess its status for next year's report.

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 2013 and in 1H14 for a sufficient length of time to be fielded and relevant solutions. 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. However, to qualify for a strong Completeness of Vision ranking, a vendor must support other platforms. 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 tradeshow 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 end-user 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. Gartner considers this certification to be a minimum standard of commitment to the encryption market. 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 2013 needed to total more than 250,000 seats — less than 1/50th of the highest reported — and 2013 LOB revenue must have been greater than \$4 million, a suitable minimum for smaller companies that have stable positions in this long-running market. Exceptions may be granted if other inclusion factors merit consideration. These thresholds were raised from the prior report.
- The vendor must provide centrally managed access controls, lockouts, and key management/recovery and system recovery methods that operate in FIPS mode.
- 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 from 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
- LOB revenue, and other basic financial and organizational metrics over a period of several years

Technologies Not Qualified for the Magic Quadrant

- Hardware encryption subsystems offered in CPUs or storage drives are enabling technologies that may be utilized by MDP products, rather than being complete solutions. Examples include Intel AES-NI and Opal SEDs.
- Embedded software encryption subsystems typically used without a full enterprise MDP management framework are not qualified for the Magic Quadrant. An example is Microsoft's Encrypting File System (EFS).
- Also not qualified are open-source projects that lack commercial support, are operated by volunteers who don't provide business-guaranteed service levels or release dates, and can end at any time. An example is TrueCrypt, a freeware, unmanaged encryption system that was favored by companies driven by cost considerations. However, the cost to create custom management for unsupported software must be considered, as well as the lack of guaranteed futures. In this case, new releases of TrueCrypt ended in 2012, and the project officially ended in May 2014.

- 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 continue. Recent surges in highly publicized breach stories continue to drive interest.

New products, new features and estimated sales in 1H14 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.

We evaluate execution categories at a constant medium weighting in order to avoid masking basic ranking values. The relative merit of each factor can be adequately expressed for the general case without additional adjustments. Readers who conduct their own RFIs may choose to change weightings to suit the needs of their business and their industry:

- **Product or 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/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, and thus is not rated.

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

Criteria	Weight
Product or Service	Medium
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Not Rated
Marketing Execution	Medium
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (September 2014)

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.

We evaluate vision categories at a constant medium weighting in order to avoid masking basic ranking values. The relative merit of each factor can be adequately expressed for the general case without additional adjustments. 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 own capabilities and partnerships with other vendors in related endpoint security markets, including antivirus, anti-spyware, configuration management, authentication, device identification, content-aware data loss prevention, digital rights management, VPNs, email encryption and gateway firewalls.

- **Sales Strategy** examines the vendor's strategy for selling products, including sales messages, techniques, marketing, distribution and channels. In this report, sales strategy is considered to be a matter of 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.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Not Rated
Marketing Strategy	Medium
Sales Strategy	Not Rated
Offering (Product) Strategy	Medium
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	Medium
Geographic Strategy	Not Rated

Source: Gartner (September 2014)

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 those of Niche Players, but not as broad as those of 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 those of 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/or 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 and deliver vision and features does not meet Gartner's prevailing view of broad competitive trends. MDP Niche Players include stable, reliable and long-term players. Market share may be limited or not easily measured. 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).

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.

All vendors and all products tracked in this Magic Quadrant offer similar basic functions, and 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, anecdotal research into matters of satisfaction and usability, favorable recognition in public settings, and appearance in RFPs. Differences in Completeness of Vision are scaled according to the breadth of the platform and the ability of a company to not only offer the features that buyers want, but also to competitively communicate the vision.

Market Overview

MDP is an established, legacy market with two primary purposes — first and foremost, to safeguard user device data by means of encryption and access control; 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 higher than the cost to invest in preventive measures, such as MDP (see "Pay for Mobile Data Encryption Upfront, or Pay More Later").

Despite ongoing high-impact breach disclosures, mitigations and fines, there is evidence that a significant number of systems are still unprotected. Most companies that invest in MDP conduct only partial installations for notebook/laptop computers, under the assumption that not all portable devices and users are at risk, and ignore most of the nonmobile systems. So there is still considerable room for new deployments and also for integration with enterprise mobility management tied to smaller devices. Gartner recommends that all companies make efforts to manage encryption across all of their endpoint platforms.

Notebook (laptop) computers running Windows OS are the most common business workstation platforms and represent the most predictable sources of revenue for MDP vendors. However, vendors cannot achieve higher vision scores unless they have broad support for multiple platforms, especially OS X, and a commitment to fully support older platforms still waiting to migrate forward, such as Windows XP and Windows 7.

Feedback from clients during the last year and a half confirms that EPP vendors have significant visibility in the MDP market and are given priority when making the MDP purchase decision. For most organizations, selecting an MDP system from their incumbent EPP vendors will meet their requirements and will result in lower pricing and fewer consoles.

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 Magic Quadrant survey results and other sources, 2013 worldwide revenue within the LOB containing MDP for vendors in the scope of this report was estimated at \$668 million, up from \$652 million in 2013 but still below \$683 million in 2012 and \$715 million in 2011, as estimated in past reports. Decreases mainly reflect discounted pricing from EPP vendors and companies that tried to get by for free by running unmanaged BitLocker and TrueCrypt installations. Slowdowns in laptop demand have an impact, but increasing public concern over data breaches, contractors and "bring your own PC/Mac" are raising the priority for MDP on laptop and desktop systems.

MDP seat sales estimates are slightly higher than in the 2013 report, but due to lack of reporting by a couple of vendors, the estimate of 46 million seats compared to 45 million last year should be considered positive. Three-year cumulative seats sold (2011, 2012 and 2013 combined) are estimated at almost 150 million, up from 119 million last year.

Extension of Existing Deployment Use Cases

While most MDP vendors have supported USB removable media encryption for many years, most continue to struggle in providing a product or even a vision for the integration of cloud-based storage environments such as Box.net, Dropbox, Google Drive and OneDrive as extensions to local file encryption capabilities. Clients looking for this level of integration should verify vendor claims by creating small proof-of-concept environments and ensuring that the level of support provided meets the client's stated intended use.

Small & Midsize (<1000 Employees) Context

🕒 16 September 2014

Analyst(s): John Girard

Mobile data protection solutions defend access to secure data on storage systems in notebooks, removable media, desktops and servers. Small and midsize businesses (SMBs) need products with affordable entry costs and minimal IT overhead.

Market Differentiators

Small and midsize businesses (SMBs) might seem to fall below the threshold for investing in strong methods for protecting and encrypting business information on workstations, including notebook/laptops and other devices. But such a decision is clearly not made on size alone. Any company that engages in business activities that fall under regulation and compliance guidelines and/or are working with valuable intellectual property must give due consideration to encryption and access controls. In a wider sense, protecting data is always the right thing to do, and no company has an excuse to ignore the issue. Real-life lessons continue to drive home the fact that laptops/notebooks, tablets and smartphones are frequently lost, stolen, misplaced or shared. The first step to protecting business information always comes down to defense of valuable but vulnerable end-user devices, and mobile data protection (MDP) addresses the solution for workstations.

Considerations for Technology and Service Selection

Market Definition for Mobile Data Protection

Gartner defines mobile data protection software as security 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. Good security practices require consistent and disciplined methods, but small businesses tend to have no full-time IT department and/or minimal staff and budget resources, which only leave room for solutions that fit within their limited financial means and IT capabilities. This research considers those resource issues when SMBs need to protect their intellectual property.

All Companies Need Proof of Compliance

The primary demonstrable value of a mobile data protection product is to prove that the company's devices, data storage and data-sharing practices comply with required policies by generating authoritative reports. SMBs may assume that large company compliance rules do not apply; however, regulations concerning issues like storage and handling of personally identifiable information (PII) are as applicable to small and midsize organizations. These smaller companies must account not only for their own obligations, but also for any that they inherit through contract work, such as medical and government projects.¹

The history of mobile data protection products began with government-grade data protection use cases. This makes implementation easier for SMBs involved in government work. For everyone else, there is no technical downside to running government-grade encryption, even if it's not mandated. The primary encryption credential is FIPS 140-2, a U.S. certification that is internationally recognized.

Installation, Upgrade and Migration Are Costly If Mishandled

Initiating encryption on a new device is relatively easy. Other devices need to be evaluated on a case-by-case basis. In the case of PCs and Macs that are already in operation, their data must be rewritten to the drives with encryption; locally, or with the aid of a backup service. Great care must be exercised when creating and running installations and migrations. SMBs may not have the staff and experience to facilitate these tasks, or the ongoing requirements for help desk support.

Free and Unsupported Tools Are Not Bargains for Limited Budgets

Free tools are missing features and will not be consistently updated or supported. Companies that follow this path will ultimately reach dead ends where the tools can no longer be upgraded or extended, and/or become more expensive to maintain than a mainstream product. A recent example is open-source TrueCrypt, which was canceled. Tools that fit in this category include various free and unsupported open source utilities, "lite/demo" versions of MDP systems, password options on word processors and spreadsheets, and various stand-alone versions of zip and outmoded utilities, such as the Windows encrypting file system (EFS), which can be only partially managed through group policies. In practice, these choices are little more than honesty systems that will be inconsistently applied by users.

Steps to Selecting a Tool for SMB Mobile Data Protection

- Contact your current value-added resellers (VARs). Many SMBs rely on VARs for operations support, so this is a logical first step. The tools most acceptable to the VAR may narrow your choices but could be the path of least resistance.
- Discuss this topic with your incumbent security vendors and learn what they can offer for MDP.

- Review the steps to install and manage encryption tools with potential vendors as part of an RFP exercise, and ask for same-size user references that will be willing to share their experiences. Ask these references about the long-term experience of dealing with updates and support.
- Consider the impact to integrate with directory services and other infrastructure to verify user credentials, bearing in mind that MDP systems can operate stand-alone if desired.
- Do not be distracted by free, lite and demo tools. Protecting mobile data protection requires money and diligence that will outlive the life expectancy of your platforms.
- Consider the impact of diversity caused by non-Windows workstations, noncompany equipment, and data shared with smartphones and tablets. For example, management from a common console may be possible, but your ability to set policies and recover diverse systems will vary.
- Don't deprioritize removable media protection as a separate purchase. This capability may be obtained from an incumbent endpoint protection (EPP) provider or the MDP provider, since nearly every one of these companies have the capability. The retail cost of stand-alone external media protection in small business quantities, even with discounts, can be as high as a full data protection suite.
- Prepare to negotiate. In seat quantities of less than 1,000, products in this market carry high published prices. As a rule of thumb, buyers should adopt the point of view that managed encryption is just another service, comparable to an investment in traditional endpoint protection, which bundles personal firewall, host IPS, anti-malware and many other features. List pricing can range more than \$100 per seat, but actual pricing can be reduced to \$10 or less depending on negotiation conditions, and bundling with other products and services.
- Expect to be pressured to adopt a free/unsupported configuration when price and complexity come under discussion.

Notable Vendors

Vendors included in this Magic Quadrant Perspective have customers that are successfully using their products and services. Selections are based on analyst opinion and references that validate IT provider claims; however, this is not an exhaustive list or analysis of vendors in this market. Use this perspective as a resource for evaluations, but explore the market further to gauge the ability of each vendor to address your unique business problems and technical concerns. Consider this research as part of your due diligence and in conjunction with discussions with Gartner analysts and other resources.

The best choice is the product or service that meets your needs for protection at an affordable price, with an acceptable level of complexity. Evaluation of the vendors mentioned below for best fit to the SMB's needs should begin with a review of the latest "Magic Quadrant for Mobile Data Protection," "Critical Capabilities for Mobile Device Management Software" (Note: This

document has been archived; some of its content may not reflect current conditions.), and by consulting Gartner analysts through the inquiry process.

1. Cloud Service Providers

Providers that offer cloud-based MDP as SaaS are an emerging choice in the MDP market, and have real advantages for SMBs that have limited resources and want to keep their IT infrastructure simple. SMBs must decide if they are willing to trust encryption installation, reporting, key management, help desk and administration to an external "storefront" service, as is often the case with antivirus/anti-malware tools. It is in fact the issue of trust that has held back the MDP SaaS market in the past.

Beachhead Solutions, a U.S.-based provider, offers cloud based MDP management services. Installation, maintenance and support are all handled remotely, a plus for the SMB with limited resources, or can be obtained through a VAR. Supported platforms include PC, Mac, flash and external drives, iOS, and Android. Pricing models include annual and monthly rates, and the first 10 devices are free. Beachhead is noteworthy for being a pure-play cloud provider.

The following vendors tracked in the Magic Quadrant have some presence in cloud services on their own or with partners and resellers. Revenue derived from cloud services is a minor part of their operations. SMBs may want to consider these vendors based on the strength of the MDP solution itself, or on the basis of a third-party relationship.

CenterTools is a Germany-based MDP provider. SaaS is available through third-party providers Leitwerk AG (Baden-Cloud), KDZ Siegen, Atos and ARZ. Revenue from SaaS accounts for less than 1% of revenue.

Check Point Software Technologies is headquartered in Israel. SaaS is available through third-party providers CSC, TeliaSonera, Vodafone and Fujitsu Services. SaaS does not generate tracked revenue.

Digital Guardian, formerly Verdasys, is a U.S.-based MDP provider. It derives a strong revenue stream from its own fully owned SaaS business, which was the highest among vendors tracked in the "Magic Quadrant for Mobile Data Protection." SaaS revenue accounts for more than 10% of revenue and is increasing.

Sophos, headquartered in the U.K., initiated a SaaS solution for MDP as this research was being completed. MDP will be blended with their existing Sophos Cloud endpoint protection SaaS.

Symantec, a U.S.-based MDP provider is offered as a SaaS solution through Aurora Enterprises, ANI Direct Network Security, Converge Net, Gradian Systems, and mindSHIFT. Revenue from SaaS accounts for less than 1% of revenue.

Trend Micro, headquartered in Japan, is resold as SaaS through AlertBoot. Revenue from SaaS accounts for less than 1% of revenue.

Wave Systems, a U.S.-based MDP provider, offers a fully owned Wave Cloud MDP SaaS solution and is seeking partners. Revenue from SaaS accounts for less than 5% of revenue.

WinMagic, a Canada-based MDP provider, is provided as a SaaS solution through ADPC, Datev and NEC Capital Solutions. Revenue from SaaS accounts for less than 5% of revenue.

2. On-Premises MDP Products

SMBs may consider all vendors tracked in the "Magic Quadrant for Mobile Data Protection" to be candidates for an on-premises solution. Historically, MDP sells well as an on-premises solution because many companies prefer to keep their encryption keys under local control. But the cost to implement on-premises MDP can be very high, especially if the number of licenses purchased is low — for example, in the hundreds of seats.

To minimize costs for on-premises systems, the SMB should look for incentives and discounts, as previously discussed. For example, your company may already have access to Microsoft's encryption and management console through other purchases. Platform providers and resellers may offer incentives, such as a free MDP trial preinstalled on new PCs, followed by a discount purchase offer. EPP vendors may offer their own MDP as reduced cost combination upgrades — for example, for companies that have a significant amount of antivirus/anti-malware already installed from a vendor that also sells EPP. Some of these "offers" may in fact have already been bundled and paid out in the original purchase and simply not recognized.

3. MDP Platform Bundles

As mentioned above, each major OS provider is a platform unto itself and offers encryption methodologies. Additionally, each PC maker provides a variety of preinstalled partner software security bundles, often with discounts and other incentives. Small businesses should look for initial discounts, free first years and other opportunities to set up for less money.

Apple provides encryption for logical and virtual disk image (dmg) files, and a systemwide agent called FileVault 2. To bring FileVault 2 into business compliance, most companies will prefer a multiplatform third-party management system over Apple's manual IT administrator tools.² Several vendors in the "Magic Quadrant for Mobile Data Protection" offer management of FileVault 2 alongside their own encryption engines.

Microsoft BitLocker embeds full volume, file and flash encryption on Windows 8 and selected editions of Windows 7. For business compliance, BitLocker can be managed by Microsoft BitLocker Administration and Monitoring (MBAM), which must be obtained as part of Microsoft Desktop Optimization Pack (MDOP), or it can be managed by several third-party vendors in the "Magic Quadrant for Mobile Data Protection" that support BitLocker alongside their own encryption engines.

Dell is unusual among PC makers for owning a MDP product. Dell Data Protection (DDP) can be purchased stand-alone and is not limited to Windows platforms or Dell PC hardware, but the best leverage for a small buyer would be based on a new PC platform bundle.

A **partial** list of additional PC maker bundles and resale agreements includes Dell (**Symantec, Trend Micro, Wave**) Fujitsu (**Wave, WinMagic**), Hitachi (**Check Point, Digital Guardian**), HP (**CenterTools, Digital Guardian, Intel Security [McAfee], Symantec, Wave, WinMagic**), IBM (**CenterTools, Digital Guardian, Symantec**), Lenovo (**Sophos, Wave, WinMagic**), Motion Computing (**WinMagic**), Panasonic (**Trend Micro, Wave**) and Samsung (**Wave**). These connections may not be available in all countries or all situations.

Evidence

¹ ["Contractors Brace for Rules on Breach Reporting,"](#) The Daily Record, 13 August 2014

² [Apple Technical White Paper: "Best Practices for Deploying FileVault 2"](#)

Gartner Recommended Reading

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

"How Gartner Evaluates Vendors and Markets in Magic Quadrants and MarketScopes"

"A Guide to Gartner's Enterprise Mobile Security Self-Assessment"

"Top Seven Failures in Mobile Device Security"

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

"Protecting Sensitive Data on Decommissioned SSDs and HDDs"

Evidence

[Common Criteria portal](#)

National Institute of Standards and Technology's ["FIPS 140-1 and FIPS 140-2 Vendor List"](#)

National Institute of Standards and Technology's ["Cryptographic Module Validation Program"](#)

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that

the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

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

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

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

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

Completeness of Vision

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

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

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

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

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

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

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS**Corporate Headquarters**

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

Regional Headquarters

AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

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

© 2014 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. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. 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](#)."