Gartner

Market Guide for Information-Centric Endpoint and Mobile Protection

Published: 19 October 2017 **ID:** G00319230

Analyst(s): John Girard, Brian Reed

Security and risk management leaders must develop a security portfolio to address different aspects of protecting information across multiple locations and contexts in a world that emphasizes connectivity, mobility, sharing and cloud, and where business information flows continuously.

Key Findings

- Data breaches involving endpoints continue to be reported at alarming rates, which clearly indicates that conventional approaches are not sufficient to protect business information in an increasingly interconnected and mobile world.
- Companies seeking business information protection tend to purchase a few point solutions that do not holistically address the range of information protection scenarios.
- Gartner has identified eight different capabilities for information-centric endpoint protection. Vendors are expanding their products to more completely address these capabilities and reduce information loss and endpoint security risks.

Recommendations

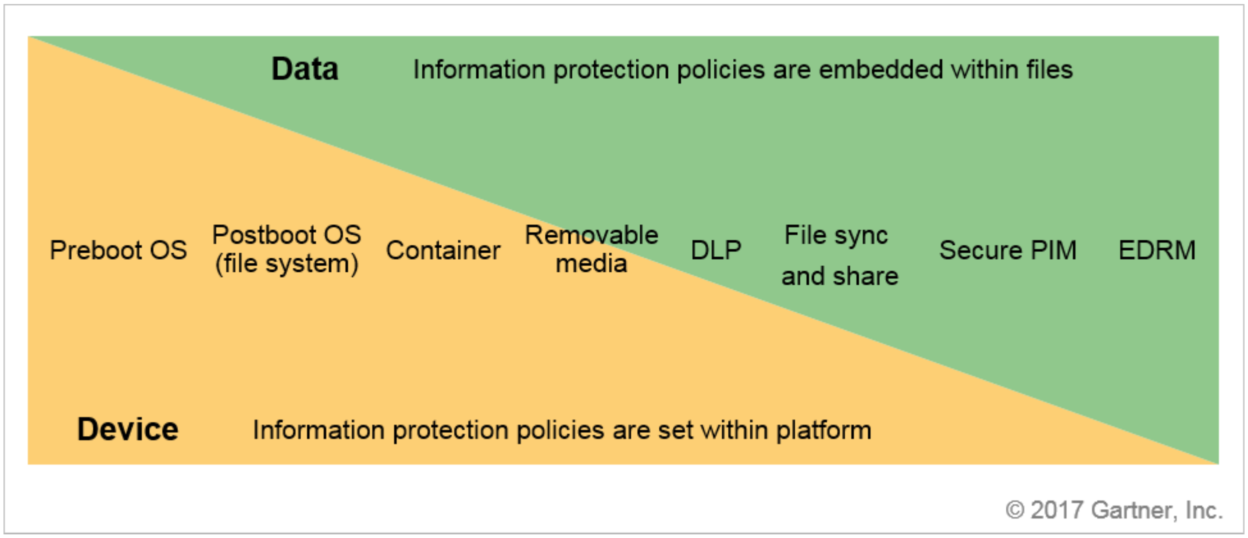
Security and risk management leaders focused on endpoint and mobile security must:

- Identify and understand the differences between different methods of protection, and the potential gaps between those methods in your organization.
- Choose products and technologies that blend information-centric protections into a "defense in depth."
- Choose vendors that invest in standards for information protection interoperability, performance and portability across protection methods, and that leverage security orchestration and automation across multiple security controls.

Market Definition

Endpoint systems are porous, mistakenly sharing data is easy, and users can be careless. Information-centric security is the last line of defense for data when firewalls, anti-malware tools, best practices and other traditional defenses fail. Products included in this Market Guide vary in their methods, but all pursue the same fundamental protection goal: to block file access from unauthorized people or circumstances. They can do this by means of up to eight different methods, as illustrated in Figure 1.

Figure 1. Comparing the Scope of Information-Centric Endpoint Protection Methods


Data
Information protection policies are embedded within files
Preboot OS
Postboot OS (file system)
Container
Removable media
DLP
File sync and share
Secure PIM
EDRM
Device
Information protection policies are set within platform
© 2017 Gartner, Inc.

Source: Gartner (October 2017)

These eight protection methods range from coarse approaches, protecting an entire disk drive, to granular ones, extending policies to individual files through rights management. In a world where information can move constantly and systems are continuously connected to the internet, products that qualify for this research encrypt and protect files at points ranging from endpoint preboot to application — for both on-device storage and for files moved to external destinations. Policies for access controls are managed centrally and can be pushed to individual endpoint systems. Rules can be set to expire access to devices, file systems and files. Endpoint devices report their statuses to verify compliance. Products in this research are software-based, and rely on endpoint device agents to maintain policies and protections. Vendors are expected to run on popular endpoint platforms, and to support industry standards for encryption, such as U.S. Federal Information Processing Standard (FIPS) 140-2 and other international certifications as appropriate, including Common Criteria (CC). All suitable embedded cryptography and accelerator techniques should be used. The list includes native crypto for Windows (BitLocker), macOS (FileVault 2), inbuilt crypto engines for iOS and Android devices, Trusted Platform Modules (TPMs) for key storage, Advanced Encryption Standard New Instructions (AES NI) for Intel CPU crypto acceleration, and self-encrypting drives (SEDs) for maximum disk response.

Market Direction

While there is not a single method to address all aspects of information protection, there is a single problem with a single desired outcome: Data losses are at an all-time high, and data breaches — both criminal actions and careless accidents — must be prevented by any and all means.

Companies are suffering from gaps in their information-centric protection, and vendors are beginning to fill those gaps, in order to stay competitive, by adopting more of the eight protection methods described in the Market Analysis section. A major success factor involves the reconciliation of keys and key management applied to different layers of encryption. Security and risk management leaders will find few comprehensive solution providers today, and should monitor the progress of vendors that show evidence of building more inclusive information-centric solutions. Consolidation means fewer layers of encryption and keys, leading to easier administration and improved scalability.

This research is updated from 2016, and is the successor to the "Magic Quadrant for Mobile Data Protection Solutions," last published in 2015. The previous definition of mobile data protection was centered on full-disk encryption (FDE). In 2016, all information is potentially mobile; disk encryption is only a piece of the solution, and protection solutions must account for the many ways that business information needs protection as it moves.

Market Analysis

Information defense technologies began as point products to solve narrow parts of the data leakage problem for buyers with limited expectations. The interconnected world and its increasingly pervasive data-sharing demands will soon force companies to put the solutions together to resolve different aspects of leakage. Full-disk and file system encryption will always play the first line of defense. Enforced protection for peripheral file transfers, such as flash drives, maintains encryption control over local ports. General-purpose containers and dedicated secure personal information managers (PIMs) provide methods to quarantine specific parts of business information workflow for particular usage patterns. Data loss prevention (DLP) and cloud file protections will trap and protect data movement to and from network resources. And enterprise digital rights management (EDRM) can imbue files with persistent encryption and access control in coordination with rights-aware apps. Each of these methods is a piece of the information protection solution. Used together, these methods overlap each other's weaknesses to reduce the risks of data leakage (Table 1).

Table 1. Eight Ways to Encrypt and Protect Business Information

Method	Protection Analysis	Failure Scenarios
Preboot OS-level encryption of physical or virtual device	The primary system disk is encrypted and protected by a preboot agent (PBA). The OS cannot boot without successful user login to the PBA. This method is optimized for single users on single workstations. Boot behavior can be modified if a device is powered up on a trusted network. **Defense value:** The OS and user data on the primary disk of a powered-down or locked device are completely unreadable.	If the system disk is unlocked after boot, then it is vulnerable to typical attack vectors. Some companies bypass the preboot agent to shorten boot time, and lose full protection as a result.
Postboot OS file system encryption	This is an alternative to full-disk encryption. This method is suitable for multiple users on shared workstations. Selective reasons to encrypt may be applied, such as folder location or file type, but this is not a DLP or EDRM solution. **Defense value:** The OS can start, but selected user files and configurations are unreadable without user login. Automated OS patch and update, as well as disk maintenance, are easier to perform, even in an unattended situation such as wake-on-LAN.	If user data can be unlocked after boot, then it is vulnerable to typical attack vectors. Protection is not guaranteed to be persistent. Selective access controls for different types of files can impact usability.
Container	Files are unreadable without successful login to a protected virtual file system. App access to container and import/export of files may be controlled. Some containers may include DLP features. This method is suitable for shared systems and multiple users. **Defense value:** Information protection is independent of OS and disk protection, and can be highly portable. Containers can be context-dedicated to specific business processes or act as a broad workspace.	User data access is determined by policy and requires that apps are configured to work in quarantined file spaces. In some cases, protection policies might be relaxed in response to usability complaints.
Removable media encryption	Files can be forced into encryption by the OS at the moment of copying to external media, such as flash drives or DVDs. Most products can keep a log of files written to flash drives. DLP-style policies can be added for specific reasons to encrypt. This method is suitable for shared removable media. **Defense value:** Information protection is independent of OS and disk protection, and can be highly portable.	The process is imperfect, as some file transfers could be missed. Once unlocked, files are difficult to impossible to track in subsequent use. Flash drives are difficult to track or remotely wipe. Other external media types may not be treated consistently. For example, a tethered phone with addressable storage may not be treated like an external flash drive.
DLP controls	File transfers can be blocked or processed with encryption based on keywords, user, project and other contexts. This method is suited to context-dependent data protection. **Defense value:** Data transfer events can be identified and evaluated using business rules and policies.	The recognition process is imperfect and made complex by the need to predefine categories of acceptable and unacceptable transfer events. In some cases, protection policies might be relaxed in response to usability complaints.
File sync and share	File transfers are processed with encryption for enterprise file synchronization and sharing (EFSS), typically involving a cloud storage service. This may be a specific application of DLP and DRM — data readability can be limited to user	The recognition process is imperfect due to the many variations of cloud sharing and backup services. Key management can be complex when

Method	Protection Analysis	Failure Scenarios
	groups, project IDs and so on. Key control over encrypted data can be held by the company rather than by the EFSS provider. **Defense value:** Data transfer events can be identified and evaluated using business rules and policies.	scaled. In some cases, protection policies might be relaxed in response to usability complaints.
Secure PIM	Secure PIMs are dedicated containment solutions that supersede default email apps, either by complete replacement or through APIs that change the encryption, forwarding, rights and other aspects of the email app itself. Many general-purpose containers can protect email files, but, in comparison, are not drop-in upgrades for secure email. **Defense value:** Email and calendar are constant security risks and are difficult to protect, especially on unmanaged devices.	Secure PIM is generally unpopular with users. In some cases, protection policies affecting email forwarding and attachment handling might be relaxed in response to usability complaints.
EDRM	This method is suited to context-dependent data protection. Files are imbued with persistent protection policies when created, read and updated. The policies can specify access by company, user, project and other details. EDRM can also stipulate limitations on app behavior, such as blocking "save as," clipboard copying, printing and so on. **Defense value:** EDRM creates the tightest possible access control relationships between files and apps. Policies can be detailed, and access can be tracked.	EDRM is difficult to scale and to apply horizontally, meaning its use can be curtailed even when otherwise mandated. A lack of standards creates interoperability problems. Rights policies with expiration dates might be tricked by backdating system calendars.

Source: Gartner (October 2017)

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Twenty-one representative vendors have been chosen for this Market Guide. Table 2 compares vendor capabilities based on the eight methods set forth in the Market Definition section. A check mark does not mean that the vendor offers a capability on all of its supported platforms. This is not an exhaustive list, and other vendors may meet business needs as well or better.

Table 2. Representative Vendors, With Information-Centric Categories Noted

Vendor and Example Product	Preboot OS	Postboot OS: File System	Container	Removable Media Encryption	DLP	File Sync and Share	Secure PIM	EDRM
Accellion kiteworks			✓		✓	✓	✓	
BlackBerry BlackBerry Enterprise Mobility Suite	✓	✓	✓	✓	✓	✓	✓	
Bufferzone Endpoint Security Solutions			✓	✓	✓			
DriveLock DriveLock	✓	✓	✓	✓	✓	✓		
Check Point Check Point Endpoint Security	✓		✓	✓	✓			✓
Dell Dell Endpoint Security Suite Enterprise, Dell Data Guardian	✓	✓	✓	✓		✓		✓
Digital Guardian Digital Guardian			✓	✓	✓			
EgoSecure Data Protection, Permanent Encryption	✓	✓	✓	✓	✓	✓		
Fasoo Enterprise DRM, eData Manager, RiskView				✓	✓	✓		✓
Ionic Security Inform, Control, Protect, Build						✓		✓
McAfee Complete Data Protection	✓	✓		✓	✓	✓		
Kaspersky Lab	✓	✓		✓	✓	✓		

Vendor and Example Product	Preboot OS	Postboot OS: File System	Container	Removable Media Encryption	DLP	File Sync and Share	Secure PIM	EDRM
Endpoint Security								
Microsoft BitLocker, Azure Information Protection, Office 365 DLP	✓	✓	✓	✓	✓	✓	✓	✓
Seclore EDRM						✓		✓
Sophos SafeGuard, Sophos Mobile	✓	✓	✓	✓	✓	✓	✓	✓
Symantec Endpoint Encryption, Information Centric Encryption	✓		✓	✓	✓	✓	✓	✓
Titus Classification Suite				✓	✓		✓	
Trend Micro Endpoint Encryption	✓	✓		✓	✓	✓		
Vera Vera						✓		✓
Virtru Virtru Data Protection					✓	✓		✓
WinMagic SecureDoc	✓	✓		✓		✓		

Source: Gartner (October 2017)

Accellion

www.accellion.com

Accellion, a California-based company, provides a secure external file sharing solution called kiteworks. Accellion kiteworks provides encryption to outbound files and can set limits on access, including authentication challenges and expiration dates. The kiteworks solution can be deployed as a private cloud on-premises (virtual appliance on-premises), as a private hosted cloud (via

Amazon Web Services [AWS] and Microsoft Azure) or as a hybrid cloud. Accellion kiteworks integrates with a wide range of third-party repositories, including Box, Dropbox, Google Drive, Microsoft OneDrive, Microsoft Exchange, Microsoft SharePoint, and others. Accellion also allows customers to create and edit Office files (Word, Excel and PowerPoint) on mobile devices. It is available on Windows, macOS, iOS, Android and Windows phone. Certifications include FIPS 140-2 and FedRAMP.

BlackBerry

https://global.blackberry.com

BlackBerry, based in Canada, offers several capabilities for information-centric protection in its Enterprise Mobility Suite. These include persistent information rights management for file and media sharing with BlackBerry Workspaces, isolation and DLP of enterprise data via application security containers with BlackBerry Dynamics, full device encryption in BlackBerry's mobility solutions suites for Android and BlackBerry 10 (BB10), FIPS 140-2 certified cryptographic software, key management (via acquisition of Certicom), secure PIM, and so on. The BlackBerry Enterprise Mobility Suite supports iOS, macOS, Android, BlackBerry 10 and Windows 10. The company holds Common Criteria EAL4+ certifications for the isolation/DLP technology for BlackBerry Dynamics apps including BlackBerry Work.

Bufferzone

https://bufferzonesecurity.com

Bufferzone is an Israel-based company that has developed a strict virtual container to protect company applications, including web browsers, email, Skype, FTP and even removable storage. Bufferzone is transparent to both the application and the end user, yet completely seals off threats from the rest of the computer. Bufferzone isolates malware and prevents it from doing harm by confining it at the boundary of the container, and it supports DLP controls for files leaving the container. Bufferzone runs on Windows.

Check Point Software Technologies

https://www.checkpoint.com

Israel-based Check Point Software Technologies, as part of its Endpoint Security product, has offered FDE and removable media encryption since 2007, using technology acquired from Pointsec. The FDE is OS-independent, using Check Point's crypto engine. Check Point's DLP software blade offers coverage of several traffic transport types, including protection for data in motion, with content-aware document security protection of mail attachments, web files and FTP. With Check Point's Document Security product, users may encrypt data on the document level for authorized users only, and, optionally, set an expiration date. Encryption can be applied automatically based on data-type classification, file location and file properties. Platform support is provided for Windows and macOS. Check Point is FIPS 140-2-certified to Level 1, and was awarded CC EAL4. Additional support is provided for Unified Extensible Firmware Interface (UEFI), Opal SEDs and Trusted Platform Modules.

Dell

www.dell.com

Texas-based Dell offers layered security solutions that include the Dell Endpoint Security Suite Enterprise. The suite includes a flexible, data-centric approach to protecting data. This is a policy-based approach that allows for full-disk or file-and-folder encryption for data at rest on system hard drives as well as removable media. Supported platforms include Windows 7 through 10, Windows Server and macOS. The add-on EDRM software, Dell Data Guardian, expands protection to data in motion and in use, also protecting data transferred through popular cloud sync-and-share services (including Box, Dropbox, Google Drive and Microsoft OneDrive) with protection that moves with the file. Dell Endpoint Security Suite Enterprise includes encryption and advanced threat prevention managed by a single console. Additional support is provided for managing BitLocker, FileVault 2 and SED deployments. The Dell suite is certified to FIPS 140-2 Level 2.

Digital Guardian

https://digitalguardian.com

Based in Massachusetts, Digital Guardian, formerly Verdasys, is a longtime content-aware player with premium tools focused on encrypting and protecting intellectual property in a DLP framework. The vendor has a global presence, but does two-thirds of its business in North America. Platform support includes Windows 7 through 10, and macOS and Linux distributions, including Red Hat, CentOS, Oracle, SUSE and Ubuntu. A fully compatible Digital Guardian app is offered for iOS. Digital Guardian core code is certified to FIPS 140-2 Level 1 and was awarded CC EAL2+.

DriveLock

https://www.drivelock.de

DriveLock, formerly CenterTools Software, based in Germany, has offered DriveLock since 2003. In addition to FDE, DriveLock File Protection offers transparent file-based encryption on removable drives, network shares and local disks. DriveLock can be configured to encrypt individual local files and folders independently of full-disk encryption. Also supported are containers consisting of encrypted virtual file systems, which can be created locally and then shared. In fact, both transparent encryption modules (file and folder and full disk) are entirely independent of each other (they can be used separately or combined). DriveLock offers access controls and transparent file-based encryption of files in common cloud-based sync clients such as Dropbox, Google Drive and Microsoft OneDrive. Platform support is provided for Windows 7 through Windows 10, macOS, iOS, Android and Linux. DriveLock owns the Gemalto (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. Additional support is provided for Intel AES NI and UEFI.

EgoSecure

https://egosecure.com

EgoSecure, based in Germany, acquired the FDE solution of Secure, a Swiss software maker, in 2014. This solution is now EgoSecure Full Disk Encryption, which is a part of the larger EgoSecure Data Protection product. EgoSecure integrates user behavior analysis (it calls Insight) with disk and file encryption solutions. Insight answers security-related planning questions in the form of clear graphs and tables, and thereby provides facts to configure the necessary encryption policies for FDE, removable media, cloud storage, folders, network shares, content filters and granular external device control. In 2017 the company added a basic portable container called Permanent Encryption. Supported platforms include Windows XP, Vista, and 7 through 10, as well as Android and iOS. EgoSecure is certified to FIPS 140-2 Level 1 in software.

Fasoo

en.fasoo.com

Based in Bethesda, Maryland, Fasoo's Data Security Framework performs discovery, classification and protection by scanning company file systems. Files are automatically classified and encrypted as they are created through desktop or server applications, or extracted from databases. Policy attributes are dynamic and travel persistently with files to control policies such as the right to view, edit, copy, paste, print, capture or decrypt. Fasoo data security products support Windows, macOS, iOS and Android platforms, and use FIPS 140-2 certified encryption modules.

Ionic Security

https://www.ionic.com

Based in Atlanta, Georgia, Ionic Security offers solutions to discover sensitive data, integrate with identity and access management (IAM), and control access to data, as well as apply encryption and rights management to unstructured data. Dynamic policies can be enforced on data generated from applications, attached to emails or documents. Ionic also publishes its API documentation and is actively working with several other vendors in the cloud access security broker (CASB) and unstructured data classification markets to integrate information protection. Ionic supports Windows and macOS, as well as Android and iOS platforms.

Kaspersky Lab

https://usa.kaspersky.com

Kaspersky Lab, headquartered in Russia, the U.K. and U.S., has provided a workstation encryption solution since 2013. Platform support is provided for legacy Windows XP and Vista, and for Windows 7 through 10. Kaspersky's endpoint protection suite and removable media protection, as well as its basic enterprise mobile management (EMM) for Apple iOS, and Google Android and Samsung Knox smartphones and tablets, are integrated in a single offering. Kaspersky has been awarded FIPS 140-2 certification for cryptography. Additional support is provided for BitLocker and AES NI. Gartner is providing buyer's guidance (see Note 1).

McAfee

https://www.mcafee.com

McAfee, based in California, provides full-disk, file-level and removable media encryption and DLP in its Complete Data Protection suites. Platform support is provided for Windows 7 through 10, and for macOS. 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.

Microsoft

https://www.microsoft.com

Microsoft, based in Washington, provides the embedded BitLocker engine to encrypt hard drives, including those on virtual machines, and external media in certain OS versions. It also offers a central management system, Microsoft BitLocker Administration and Monitoring (MBAM), for companies that are licensed for Microsoft Desktop Optimization Pack (MDOP). Manageable file-level encryption that enables data separation and containment is now offered through Windows Information Protection (WIP), which was added to the Windows 10 Anniversary Update. Microsoft Azure Information Protection (AIP) provides classification assistance as files are created or modified. Office 365 DLP and message encryption work across Office apps, as well as Exchange email, SharePoint and OneDrive. A component of Intune is needed to fully enforce managed app DLP policies on iOS and Android. Microsoft Rights Management Service (RMS) applies persistent policies to files to control use rights, copying, saving and so on. RMS AIP works across Windows, macOS, iOS and Android, and can protect all types of files. RMS AIP is validated to FIPS 140-2 Level 2 when combined with hardware security modules. BitLocker and MBAM are certified to FIPS 140-2 Level 1 in software. There is additional PC support for TPM, UEFI and Opal SEDs.

Seclore

www.seclore.com

California-based Seclore facilitates security in external collaboration. Seclore provides persistent and format-/device-/sharing-independent security for documents and email. The solution includes standard EDRM features, such as native app access, classification support, revocation, and information-centric audits. OS support includes Windows XP to 10, macOS, iOS and Android. Advanced features are also provided, such as location-based controls for data residency requirements, pluggable encryption, bring your own key (BYOK) and FIPS-140-2-compliant encryption. Files downloaded from any enterprise application can be automatically protected with the source system security policies. Seclore maintains more than 80 connectors for identity and single sign-on (SSO) systems, including but not limited to Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), OAuth, enterprise content management (ECM) and EFSS (such as Box, Citrix ShareFile, IBM ECM, Microsoft SharePoint and Dell EMC Documentum), messaging systems (including Microsoft Outlook, IBM Notes, and Gmail), DLP systems (including Symantec and McAfee), transactional and analytics systems (such as SAP and SQL Server Reporting Services [SRSS]), and security information and event management (SIEM) systems (including Hewlett Packard Enterprise [HPE] Security ArcSight, and Splunk). An API is offered to develop additional connectors. Supported platforms include Windows (from XP through 10), macOS, iOS and Android. Encryption is certified to FIPS 140-2, and SAP has certified "Seclore Rights Management for SAP."

Sophos

https://www.sophos.com

Sophos, headquartered in Oxford, U.K., offers SafeGuard Encryption, a hard drive, external media and file encryption product built on technologies originally acquired from Utimaco. Platform support is provided for Windows and macOS, and iOS and Android. Sophos Mobile provides additional file encryption, container and secure PIM functionality on iOS and Android. File-based encryption can be set up as an alternative to FDE or to run in parallel. The company's design for "synchronized encryption" adds DLP and persistent DRM protections for files transferred between devices and external destinations, such as USB and EFSS, including policies for read, write, save and so on. Protected files can be placed in HTML5 encryption wrappers at the time of transfer to external storage or email for collaboration external to the organization. Sophos is certified to FIPS 140-2 Level 1, 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.

Symantec

https://www.symantec.com

California-based Symantec offers Information Centric Encryption (ICE) service and Symantec Endpoint Encryption (SEE). ICE protects files in the cloud and on-premises, as well as mobile files, facilitating internal and external collaboration. It can also remotely delete sensitive documents. ICE can also provide access to documents with Touch ID. SEE provides preboot OS hard drive and removable media protections. Symantec Desktop Email Encryption and Symantec File Share Encryption will block unauthorized file transfers and protect approved files and folders in transit. Platform support includes Windows 7 through 10, and macOS and Linux distributions, including Ubuntu, Red Hat Enterprise Linux (RHEL), CentOS, SUSE and SUSE Linux Enterprise Server (SLES). Also supported are FileVault 2, Intel AES NI, BitLocker and Opal SEDs. Symantec products use FIPS 140-2 Level 1-validated cryptography. Parts of the solution, for example PGP encryption, are Common Criteria-certified.

Titus

https://www.titus.com

Titus, a Canadian-based company, provides data discovery, classification and DLP to secure email, documents and other file types on workstations, mobile devices and cloud services. Titus Classification Suite scans and applies metadata to unstructured information and supports automatic or user-led classification. Titus Illuminate scans and inventories on-premises file shares, Box, Dropbox, Microsoft OneDrive and Microsoft SharePoint; classifies and optionally encrypts the files it discovers; and provides a data inventory for analysis. Titus Classification for Mobile provides email classification and a secure container for business documents, with direct access to corporate SharePoint libraries and common cloud sharing services. Titus interoperates with Microsoft RMS and Ionic Security, preserving access rights to encrypted files. Titus extends Microsoft RMS to mobile devices, allowing users to access email and files protected using Microsoft RMS.

Trend Micro

https://www.trendmicro.com

Trend Micro, based in Tokyo, offers an FDE drive and removable media encryption built from technologies acquired from Mobile Armor in 2011. In addition, it offers integrated DLP controls, cloud file encryption and email encryption. These, as well as other endpoint protection platform capabilities, are offered as part of the Smart Protection for Endpoints suite and are managed under a common console. Platform support is provided for Windows 7 through 10, macOS, iOS and Android. Linux is also supported for email encryption on the gateway. 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 SanDisk, Opal SEDs, TPM, and Intel AES NI.

Vera

https://www.vera.com

Based in Palo Alto, California, Vera offers information protection for unstructured data and email body and attachments, and integrations for Box, Dropbox, Microsoft Office 365 (e.g., Office, SharePoint, SharePoint Online and OneDrive for Business), local file stores, and endpoint storage. Vera policies and permissions can be set automatically or managed directly by content owners, and can be dynamically updated without having to reissue files or certificates. External collaborators are not required to download an application or plug-ins to access content, and Vera's solution is agnostic to the underlying storage platform or application. The Vera platform also provides access to functions to secure, track and manage access to content through a REST API and software development kit (SDK) within custom applications. Vera's SDK supports applications running on Windows, macOS, iOS, Android, and Linux operating systems.

Virtru

https://www.virtru.com

Based in Washington, D.C., Virtru supports information-centric protection across both Google and Microsoft applications through encryption of content using the Trusted Data Format (TDF), an open standard for cross-platform, persistent data protection. Policies and protections can be applied across Windows, macOS, iOS and Android operating systems, and integrated within Google applications including Gmail, and Microsoft applications, such as Office 365, Outlook and Exchange. The Virtru data protection platform also allows customers to secure communications from SaaS business applications like NetSuite, Salesforce and Workday. The Virtru Customer Key Server enables encryption keys to be hosted on-premises or in a cloud service.

WinMagic

https://www.winmagic.com

WinMagic, based in Canada, offers comprehensive encryption solutions for workstations, virtual and cloud platforms. SecureDoc is geared toward businesses with high security needs and compliance requirements. Platform support for endpoints is provided for macOS, Windows 7 through 10, Windows Server and Linux distributions, with additional support for TCG Opal and Enterprise SEDs. Support for virtual and cloud platforms includes VMware vSphere, Citrix Xen, Microsoft Hyper-V, AWS Elastic Compute Cloud (EC2), Microsoft Azure Virtual Machine, IBM Cloud, Nutanix and Scale Computing. Extensions will protect data across local files, network file shares and EFSS services. Advanced boot control features are provided through PBConnex for network preboot, and a strong replacement preboot process for BitLocker and FileVault 2, as well as location-based controls for data residency in the cloud. Additional support is provided for dm-crypt, TPM, Intel AES-NI, and UEFI. WinMagic is certified to FIPS 140-2 Level 1 and was awarded CC EAL4.

Market Recommendations

Security and risk management leaders who grapple with endpoint security challenges must accept that astute information protection requires a blending of several methods. Table 2 shows the capabilities of information-centric protections of listed vendors. Security planners can use this to track the breadth of information protection solutions and choose the vendors that best fit their needs.

Endpoint devices will continue to be an attractive focus for hackers for harvesting business data. These devices are real, tangible, accessible and abundant. The users of these devices will also continue to make human errors that cause information to be vulnerable.

Disk encryption remains the oldest and best defense against extraction from a lost, stolen or mishandled endpoint device. At the opposite extreme, EDRM promises to be the most flexible and pervasive future technique to protect files regardless of where or how they are shared. In between these extremes, choices should be made that match current information security concerns. For example, USB flash drives have taken on a role similar to paper, and are often handled carelessly. If a company cannot ban flash drives, then encryption controls should be added. If the primary reason for access through BYO devices is to receive email and calendar, then a secure PIM can give security and risk management leaders some much-needed lead time to explore other options. Review the defense value summaries in Table 1 and choose accordingly.

Information theft pays big benefits to thieves, and plagues businesses with long-term damage. It is the "hack that keeps on giving," since the extent of breaches is not always known, and business information can have long-term exploit value, extending into years — and lifetimes in the case of some medical and financial knowledge. Once thieves have obtained your business information, they can unplug from your systems and they will be difficult to trace.

Gartner Recommended Reading

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

"Data Can Move Without Leaking — Eliminate Four Flaws in Your Mobile Information Protection Strategy"

"It's Time to Redefine Data Loss Prevention"

"Market Insight: The Future of Data Security"

"Getting Your Organization Ready to Deploy Enterprise Digital Rights Management"

"Comparing Options for User Endpoint and Mobile Device Encryption"

"Critical Capabilities for High-Security Mobility Management"

"Hype Cycle for Mobile Security, 2017"

"How to Live With Unmanaged Mobile Devices"

Note 1 Buyer's Guidance on Kaspersky

If the business risk of the Russian government, intelligence or police agencies getting access to metadata from your organization is significant, or the reputational risk to your organization from using Kaspersky Lab software is manifest, or if it puts in peril the organization's ability to work with the U.S. federal government, then it is prudent to consider switching to another antivirus solution aligned with business goals. Otherwise, Gartner suggests monitoring the situation closely to see if any evidence of data leakage or other issues emerges.

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