Comprehensive Data Protection

October 2013

Overview

According to Gartner, there are four factors driving interest in data protection solutions: regulatory compliance, intellectual property protection, risk management, and proof of data protection. Here are some examples of customer pain points.

In the Customer's Words

We need to protect our organization's data, brand, and reputation. We're required to protect compliance-related data. We need to protect our intellectual property. If a data breach occurs, we need to know who had access to data, and we must be able to prove that security, access controls, and processes were in place prior to the event.

For More Information

After reviewing this guide, to get additional questions answered, visit the Sales Portal , McAfee.com, or contact Cindy Chen, Senior Manager Product Marketing DLP, 408-346-3852, Cindy_Chen3@McAfee.com

---

Table of Contents

Overview	2
Target Markets	2
Compelling Event/Drivers	3
Qualifying the Opportunity	3
Qualifying Questions	5
Solution Defined	6
Competitive Analysis	7
Customer Success Stories and Partners	8

Overview

Regulatory compliance — How can I meet the requirements and demonstrate compliance with the various laws and industry regulations affecting my organization, such as:

- *HIPAA/HITECH for Healthcare*
- *PCI for Retail*
- *Gramm–Leach–Bliley Act (GLBA) and Sarbanes-Oxley (SOX) for Financial Services*
- *International Traffic in Arms Regulations (ITAR) for High Technology and BioTech/Pharmaceuticals*

Intellectual property protection — I have a complex business environment with operations in regions without strong intellectual property protection. I have hundreds of mobile workers who have mobile devices that store or access confidential company information. We have invested millions in R&D, creating valuable intellectual property that must be protected. I don't want any of this critical company information to get into the wrong hands. How can I keep the intellectual property secure while sharing it with those who need the information in order to do their jobs?

Risk management — I don't want my company to be in the news for a data breach because we didn't take the necessary steps to protect our sensitive data. Our data is everywhere —perhaps unencrypted on end-user endpoints, most of which are highly mobile. How do I ensure that valuable company data remains secure and that we comply with regulations and avoid fines while protecting the brand? My company is reorganizing — how do I monitor high-risk or impacted employees?

Proof of data protection — I don't want my organization to face legal action, financial penalties, or loss of competitive advantage for not taking appropriate steps to prevent leakage of sensitive data. I'm safeguarding data using encryption and data loss prevention (DLP). How can I prove that I have robust processes in place to protect my data? How can I prove that my protection is working?

Target Markets

Target Markets: DLP

In general, the "sweet spot" for deals involving McAfee Data Loss Protection (DLP) is companies with 1,000 or more employees. While there are a few exceptions, this is what we should be focusing on given that these are high-touch sales, with a relatively long sales cycle (six months).

Additionally, target organizations are those that are subject to regulations (e.g., PCI for Financial Services, HIPAA for Healthcare, and so on), and have signification intellectual property to protect (e.g., High Technology, Biotech, and Pharmaceuticals).

Target Markets: Endpoint Encryption

The target market for endpoint encryption is much broader and the sale is much less complicated than DLP. For encryption, the target is any business, government, or organization with workers that use, share, store, or access company confidential data using desktop computers, laptop computers, servers, and/or removable media like CDs and USB drives. For the encryption aspect of this sales playbook, the target is organizations with 500 or more employees.

Personas: DLP

To successfully sell DLP, a number of different stakeholders must be involved.

Internal influencers — internal influencers are the most important stakeholders because they drive the need for DLP. Examples of internal influencers are:

- *Chief executive officers (CEOs), chief information officers (CIOs), chief information security officers (CISOs), chief financial officers (CFOs), chief risk officers (CROs), and chief learning officers*
- *Legal, human resources, compliance, privacy, and marketing business unit heads,*
- *Directors of messaging, desktop operations, network operations, and security operations — these stakeholders will most likely evaluate the technical capabilities of the solution. Stability, ease of use, and other key features are important to them.*

Target buyers — while the internal influencers drive the need for DLP, the target buyers are the stakeholders who are responsible for the security budget. These are also the groups who will be responsible for maintaining the solution. Example titles for these stakeholders are VP of infrastructure, VP of security, VP of desktop operations, and VP of network operations.

Personas: Endpoint Encryption
Here are the target key decision makers and stakeholders who should be involved in encryption solution purchases:

- ***CISO/CIO —*** *senior level executives who focus on information security and compliance within an organization.*
- ***VP/director of desktop operations —*** *The VP/director of desktop operations directs desktop operations to provide the organization's workers with the highest quality customer service and technology-based solutions and systems, in the most cost-effective manner, enabling company workers to meet business goals.*
- ***VP/director of compliance/privacy —*** *The VP/director of compliance/privacy directs the corporate compliance program, an independent, objective body that reviews and evaluates compliance issues/concerns within an organization.*
- ***IT manager (operations, mobility, messaging, and/or security) —*** *The IT operations manager manages existing operations and implements new operations processes. The information security manager provides appropriate access to company information and protects the confidentiality and integrity of customer, employee, and business information in compliance with the organization's policies and standards.*

Compelling Event/Drivers

Here are some compelling events that cause customers to invest in data protection:

- *The organization has mandatory compliance requirements.*
- *The organization is going through a reduction in force (i.e., layoffs) and is concerned that departing employees will steal confidential information.*
- *A competitor is constantly one step ahead — the organization is wondering if someone on the inside is leaking launch plans.*
- *A breach of confidential data occurred in the organization — now they need to employ a security solution to prevent future breaches and protect the organization from legal action.*
- *A news story reports a data breach that has negative repercussions for a large, well-known company — many organizations decide it is time to implement a security solution before their data is compromised.*
- *Integration with McAfee DLP solutions.*

Qualifying the Opportunity

DLP — Gartner projects the standard of due care will include content-aware DLP in North America by 2013, Europe by 2015, and a minimum of four Asia Pacific countries by 2015.

Endpoint Encryption — Per the Gartner Magic Quadrant for Mobile Data Protection 2013 available through http://www.mcafee.com/us/independent-reports/gartner-mq-mobile-data-protection.aspx (that focuses primarily on encryption for mobile data on computers and devices):

- *Gartner "recommends all companies make efforts to broadly install encryption across their workstations."*
- *Gartner states, "Most companies, even if not in sensitive or regulated industries, recognize that encrypting business data is a best practice."*

Trend One: Regulatory Compliance

Inside the regulatory realm, the major compliance driver is the PCI-DSS. Gartner's conversations with DLP customers indicated that in many instances locating repositories of credit card information and controlling the flow of this information have been major factors in the decision to implement content-aware DLP technology.[1] For HIPAA/HITECH, for example, the U.S. Department of Health and Human Services (HHS) guidance specifies "…encryption and destruction as the (only) technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information" (Source: hhs.gov, Nov 2011). For a comprehensive, searchable view of U.S. and international laws and regulations, visit www.mcafee.com/us/regulations/index.aspx.

[1] *Four Factors Driving Interest in Content-Aware Data Loss Prevention: A DLP Spotlight. Eric Ouellet, Rob McMillan. June 2011.*

Customer Pain Point for Trend One:

- *How can I demonstrate that I am compliant with various laws and industry regulations affecting my organization (e.g., HIPAA/HITECH for Healthcare, PCI for Retail, GLBA and SOX for Financial Services, and ITAR for High Technology and BioTech/Pharmaceutical)?*

Qualifying Questions for Trend One:
What regulations does your organization have to comply with?

- *How can you demonstrate that you are compliant with various industry regulations (e.g., HIPAA/HITECH for Healthcare, PCI for Retail, GLBA and SOX for Financial Services, and ITAR for High Technology and BioTech/Pharmaceuticals)?*
- *How could you benefit from having tools to help you deal with the multiple regulations your company must comply with? For example, the GLBA requires that nonpublic personal financial information be protected. How are you ensuring that this is indeed the case?*
- *What was the overall cost of the breach/attack?*
- *If you could spend less time and resources managing regulatory compliance, how would you use the savings?*
- *How could you benefit from having tools to help you deal with the multiple regulations your company must comply with?*
- *How would you benefit from being able to reliably pass audits?*

Trend Two: Intellectual Property Protection

Enterprises are increasingly sensitive to the need to maintain the value of their IP by controlling access to it as well as its distribution and use. This is becoming a more important issue, due to the growing complexity of the business environment and particularly because of global supply chains, which frequently include operations in regions without strong IP protections. IP can take many forms, including negotiated contracts or settlements, product specifications, service manuals, analyses, chemical formulas, computer-aided design (CAD)/computer-aided manufacturing (CAM) files and many other documents. Content- aware DLP is a critical element in any enterprise strategy for IP protection. Gartner recommends the broad use of endpoint encryption and specifically calls out encryption as a best practice.

Customer Pain Point for Trend Two:

- *I have a complex business environment with operations in regions without strong intellectual property protection. I have hundreds of mobile workers who have devices that store or access confidential organizational information. My organization has invested millions in R&D, creating valuable intellectual property that must be protected. I don't want any of this critical company information to get into the wrong hands.*

Qualifying Questions for Trend Two:

- *How do you know that all your sensitive data is protected?*
- *How can you be sure that you know where all your sensitive data is stored and who has access to it?*
- *If a data breach occurred, how would you know what was lost? Would you know how was it leaked, when the problem started, and who was involved?*
- *Most companies have no way of knowing what caused a data breach. How would you benefit from being able to complete thorough investigations in dramatically less time?*
- *How do you ensure that only authorized users have access to your sensitive data?*
- *How would you know if your intellectual property made it into the wrong hands?*
- *Would it be valuable for you to see who has accessed your confidential data over the last 48 hours?*
- *What processes do you have in place to ensure that you are not in violation of ITAR and/or Office of Foreign Asset Control (OFAC) regulations?*
- *How can you maintain the value of your intellectual property while sharing it within the global supply chain?*

Trend Three: Risk Management

The risks — financial, regulatory, and reputational — associated with the mishandling of some classes of information can be extremely high, placing significant pressures on organizations to properly handle and limit access to sensitive data. Content-aware DLP is a useful tool to monitor and control access to sensitive information, allowing companies to reduce the risks associated with inappropriate data disclosure. Encryption makes data unreadable and indecipherable to unauthorized individuals.

Customer Pain Point for Trend Three:

- *I don't want my company to be in the news for a data breach because we didn't take the necessary steps to protect our sensitive data. Our data is everywhere — perhaps unencrypted on end-user endpoints, most of which are highly mobile.*

Qualifying Questions for Trend Three:

- *How will you ensure that valuable company data remains secure?*
- *How will you ensure that you comply with regulations and avoid fines while protecting the brand?*

Trend Four: Proof of Data Protection

Enterprises facing various types of legal action, including claims based on data loss, can use DLP tools for e-discovery to support their positions. Furthermore, the existence of an established DLP process, even if it does not provide specific support, can be useful in determining the balance of probabilities in civil cases. Organizations defending against allegations about the leakage of information may be able to use DLP records to show that a formal, robust, and reliable detection process is in place, and that either (1) a given event did occur by virtue of an existing record, or (2) a given event is unlikely to have occurred, due to the absence of a supporting record in an otherwise sound process that would have detected and recorded such an event.

McAfee Endpoint Encryption solutions — McAfee Endpoint Encryption solutions leverage the McAfee ePolicy Orchestrator (McAfee ePO) platform to provide actionable intelligence, auditing, reporting, and proof of protection.

Customer Pain Point for Trend Four:

- I don’t want my organization to face legal action, financial penalties, or loss of competitive advantage for not taking appropriate steps to prevent leakage of sensitive data.

Qualifying Questions for Trend Four:

- *How can you prove that you have robust processes in place to protect your data?*
- *How can you prove that your protection is working?*
- *How can you be sure that you know where all your sensitive data is stored and who has access to it?*
- *Most companies have no way of knowing what caused a data breach. How would your company benefit from being able to complete thorough investigations in significantly less time?*

Qualifying Questions

Here are some examples of qualifying questions:

- *What regulations does your organization have to comply with?*
- *How do you know that all your sensitive data is protected?*
- *If you had a breach, would you know what caused the breach?*
- *How would you know if your intellectual property made it into the wrong hands?*
- *If a data breach occurred, how would you know what was lost? Would you know how was it leaked, when the problem started, and who was involved?*
- *How can you be sure that you know where all your sensitive data is stored and who has access to it?*
- *What processes do you have in place for classifying data?*
- *How beneficial would it be for you to be able to monitor how data is used without imposing restrictions?*
- *How are you ensuring that your confidential data is stored in secure/encrypted locations?*
- *How important is it to you to have consistent enforcement of data protection policy?*
- *Did you know that the leading analyst firm Gartner stated that all companies need encryption?*

Solution Defined

Value Proposition — DLP

McAfee DLP provides business-centric data protection by safeguarding intellectual property and ensuring compliance for all sensitive data, regardless of location — whether it is on premise, on your mobile endpoint, or in the cloud.

McAfee's unique Capture technology helps you build better data security policies faster by giving you visibility into how your sensitive information is being used across the enterprise.

The McAfee DLP data classification capability can reduce the risk of a breach in enterprises with hundreds of servers, thousands of file shares, and millions of data objects by rapid data inventory and categorization, and automated remediation.

Value Proposition — Endpoint Encryption

McAfee Encryption solutions protect valuable data on end-user devices with comprehensive encryption and centralized management, shared policies, robust reporting and proof of protection. Productivity increases while protecting data on desktop PCs, laptops, smartphones, shared platforms, networks, and removable media.

The McAfee ePolicy Orchestrator management infrastructure masterfully enables centralized deployment, management, policy administration, password recovery, monitoring, reporting and auditing for ease of management, consistent protection, and low total cost of ownership (TCO).

Leading analyst firm Gartner has positioned McAfee as a Leader in the Gartner Magic Quadrant for Mobile Data Protection for 6 consecutive years and receives highest position for ability to execute and completeness of vision. See http://www.mcafee.com/us/independent-reports/gartner-mq-mobile-data-protection.aspx

Key Products — DLP

The following products/suites support this sales play.

- *McAfee Total Protection for Data Loss Prevention (DLP), which is comprised of:*
- *McAfee DLP Discover*
- *McAfee DLP Monitor*
- *McAfee DLP Prevent*
- *McAfee DLP Endpoint*
- *McAfee DLP Manager*
- *McAfee DLP Device Control*

For DLP, the goal of this sales play is to sign up the customer/prospect for a McAfee 48-Hour Data Risk Assessment, which will be delivered by a channel partner. Our experience shows that in opportunities where a risk assessment is performed, 70% to 80% are converted into a sale.

Key Products — Endpoint Encryption

The key products for endpoint encryption are:

- ***McAfee Drive Encryption:*** *full disk encryption for Microsoft Windows computers and Apple Mac computers (not sold indivdually, available only in CDA or CDB suites).*
- ***McAfee File & Removable Media Proteciton :*** *encryption for files and folders on end user devices and/or multiuser serverss, supports removable media and portable storage devices like USB flash drives and CD/DVD (not sold individually, available only in CDA or CDB suites).*
- ***McAfee Enterprise Mobility Management*** *(EMM) - provides security and mobile device management for smartphones and mobile devices.*

The suites that include encryption are:

- ***McAfee Complete Data Protection - Advanced (CDA)*** *– Drive Encryption, File & Removable Media Protection, ePO Deep Command, DLP Endpoint (including Device Control)*
- ***McAfee Complete Data Protection (CDB)*** *– Drive Encryption, File & Removable Media Protection, ePO Deep Command*

- ***McAfee Total Protection for Endpoint — Enterprise Edition (TPE)***
- ***McAfee Total Protection for Secure Business (TEB)***

The sales play goal for endpoint encryption is to get customers/prospects to purchase and install McAfee endpoint encryption solutions for their highest risk endpoints first (i.e., laptop computers used by employees and executives who work offsite full-time or part-time), and then deploy broadly across the organization. The target is organizations with 500 or more employees.

Competitive Analysis

Competitive Positioning — Data Loss Prevention

Competitor	Weaknesses
Symantec	**The Symantec solution does not provide these McAfee capabilities:** • *Symantec DLP needs multiple consoles/agents for full DLP support. In addition, it requires a separate Oracle and SQL Database requirements which leads to higher cost and complexity. McAfee DLP solution is much simpler to deploy and manage.* • *Symantec's Vector Machine Learning is an unreliable technology that has failed vendors in the past. The flaw in Vector Machine Learning technology lies within the trained positive/negative data and the manual process of keeping the training database updated* • *Symantec DLP Endpoint requires a separate agent on the endpoint in addition to is AV. Extra agents mean more latency and less employee productivity. McAfee DLP Endpoint works with McAfee AV as a single agent on the endpoint and can be centrally managed by ePO, less latency = more productivities.*
Websense	• *Websense Data-in-Motion classification is limited to web and email; there is no general network monitoring. It does not have network control for IM protocol; no network visibility on NNTP traffic, P2P Traffic, telnet traffic, and TCP ports. McAfee is able to protect data over a much greater range of network protocols* • *Websense went private recently after consistent financial troubles. It just went through major management turnover. The private equity firm Vista's portfolio does not include any other security companies. Websense will likely just be overhauled financially, rather than shifting strategy.* • *Websense has to create separate policies for data-at-rest and data-in-motion, requiring duplicate effort. In addition, Websense does not offer discovery for generic HTTP/FTP nor support the scan of Documentum. Websense discovery policies are alert only and have no quarantine functionality. McAfee's DLP can be managed via ePO which gives controls alongside other endpoint related settings.*
RSA	• *RSA is unable to index and keep track of data that does not trigger a policy for use with Data Discovery. RSA requires for prior knowledge of sensitive data in order to implement efficient DLP policies.* • *RSA continues to have basic endpoint agent. Its clients reported performance and accuracy issues with using some of the advanced content fingerprinting capabilities on the endpoint.* • *RSA's DLP endpoint agent continues to be basic. RSA clients reported performance and accuracy issues with using some of the advanced content fingerprinting capabilities on the endpoint. Also, RSA lacks integrated DLP agent deployment and relies on 3rd party tools such as SCCM or other endpoint management system*

Competitive Positioning — Endpoint Encryption

Competitor	Weaknesses
Symantec, PGP, and GuardianEdge	• *Unlike McAfee solutions, the Symantec, PGP, and GuardianEdge solution is not integrated.* • *The Symantec, PGP, and GuardianEdge combination has no integration, multiple separate consoles, and poor deployment tools.* • *Unclear support and integration roadmap for existing PGP, GuardianEdge, and Symantec Endpoint Encryption users.* • *Unclear device control roadmap and integration strategy.*
Sophos	• *No integration between SafeGuard Enterprise (SGE) and Sophos Enterprise Console (SEC)* • *No integrated file and folder encryption with SGE* • *No enterprise level DLP solution; compatibility and integration issues between components have caused many "blue screens"*
Check Point	• *Check Point still requires three consoles to manage full-disk encryption, removable media, and endpoint secure access* • *No web-enabled central console or central deployment capability; poor reporting; no host data loss prevention (HDLP); no file and folder encryption*
Microsoft	• *Limited OS support* • *No safe harbor—unable to provide proof of protection* • *Not really free—there are hidden costs*

Customer Success Stories and Partners

Banco de Crédito e Inversiones (BCI) — Leading Chilean bank with over 10,000 employees needed to comply with PCI DSS. The BCI was concerned that employees might steal customer information when they changed employers, sell or misuse data fraudulently, or put information at risk in any number of innocent but misguided ways. McAfee DLP allows the BCI to do a better job at protecting confidential customer information, blocking errant employee behavior that the bank was previously aware but unable to stop, all without impacting daily business processes.

Energy company — A large, U.S. independent gas and oil producer with over 7,000 employees, decided to sell one of its divisions and was worried that some employees might leave the company and take confidential data to their next employer. The company knew it needed to protect this data quickly, but did not have data protection solutions in place. Even worse, it was unequipped to even understand what data was in need of protection, where it resided, and where it went when it was moved. The company launched an urgent process to classify data and is using the complete McAfee DLP suite – DLP Monitor, DLP Discover, and DLP Endpoint — to successfully classify and protect data.

MedStar Health — MedStar Health, a North American healthcare provider with over 30,000 IP addresses, found that access to inappropriate sites was an ongoing issue despite the presence of blocking technologies. Using McAfee DLP, MedStar Health created a policy that looks for images with skin-tone variations because they could indicate access to inappropriate websites. If access to an inappropriate website is suspected, the staff can investigate and track where the images traveled anywhere throughout the internal network.

Fortune 50 pharmaceutical company — a large pharmaceutical company did not know that intellectual property in the form of drug research and drug trial information was leaving the organization. The research department heads were too busy to worry about IT, but the IT director knew the code names for all the drug research projects. After monitoring corporate-wide information flows, he was able to go back to the department heads with proof of how the information was leaving the company and with recommendations on how to prevent future losses. The IT director is now CSO and candidly shared with us that his ability to go back to the business with answers and recommendations, not questions, was what eventually propelled his career from IT director to CSO.