McAfee Data Loss Prevention (DLP) At-A-Glance

Customer Problem/Challenges

- Increasing global and regional regulatory compliance requirements
- Lack of visibility into sensitive data - where they live and how they are used
- Limited DLP knowledge and expertise leads to lengthy, resource-intensive deployments that delay protection

Target Customer/Profile

Segments:
Enterprises with 1,000+ employees
Industries:
Healthcare, Pharmaceutical, Finance, Public Sector, Energy, High Tech
Key Titles:
Chief Security Office, VP of Information Security, Director of Risk and Internal Control, Chief Compliance Officer

Value Proposition

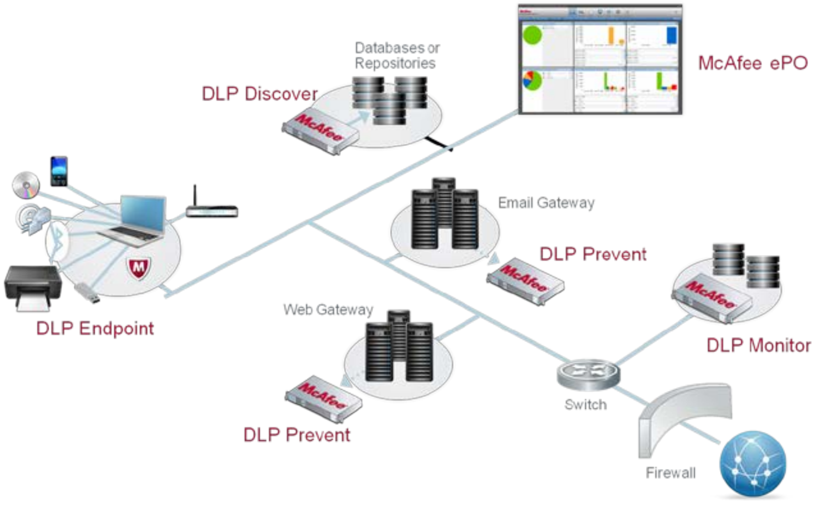
In a business environment where new privacy regulations are appearing all the time and malicious and inadvertent threats can come from both outside and within an organization, you need a comprehensive and cost effective solution to maintain compliance and protect company IP.

McAfee DLP solution safeguards IP and ensures compliance by protecting sensitive data wherever it lives – on premise, in the cloud or at the endpoints. Its unique Data Classification and Capture Technology speed deployment and time to value by enabling you to more effectively identify, categorize, and remediate sensitive company information.

Key Sound Bytes

- *Enhanced protection against data loss on the network and endpoints*
- *Accelerated deployment and time to value*
- *Increased visibility into all data and how it is used*
- *Improved compliance and security of intellectual property*

McAfee Solution



Feature	Function	Benefits
Capture Technology	Provides a historical record of all data leaving the enterprise, without interrupting business.	Builds better DLP policies faster and more accurately.
Data Classification	Classifies large amount of data on servers and file shares with rapid data categorization & remediation.	Saves time and resources by categorizing so only relevant files are being remediated.
Location and Application Tagging	Tags all the files that are coming from a protected location or application.	Sets up simpler policies for data without crawling through the servers and fingerprinting every single file.
Virtualization Support	Supports Citrix and VMware terminal server (VDI) and Microsoft Terminal Server.	A per-user policy which allows flexibility and better control of the data flowing to
Unified DLP management via ePO	Manages both DLP Endpoint and Network DLP polices and incidents.	Saves time and costs with centralized management console.

Awards/Recognition

Gartner

In Gartner DLP Leader's Magic Quadrant since 2008

"The capture database, which allows for data captured previously to be used for analysis and testing new rules, is an innovative and distinctive feature that has been well received by clients."

McAfee Data Loss Prevention (DLP) At-A-Glance

McAfee An Intel Company

Conversation Flow

Greeting: "Hello, this is ___ with ____. I was calling to discuss the capabilities of the McAfee DLP solution and how it can help you protect your most valuable information from accidental or malicious loss. Do you have a few minutes?"

Question 1: "What internal controls do you have in place today to prevent data loss, and are you confident in their ability to help you pass compliance audits?"

Question 2: "When you think about protecting sensitive data in your organization, what is your primary concern?"

Question 3: "Have you ever experienced a data loss event triggered by a well-intentioned employee who made a careless mistake?"

Wrap Up: "I'd like to set up a time for you to meet with one of our data protection specialists, view a demonstration of the McAfee DLP solution, and receive a fast benefit analysis of how it can help your organization meet regulatory compliance and protect sensitive data while lowering the cost of operations."

Objection Handling

Objection	Response
1. Already using another vendor's DLP	Are you confident that the solution is protecting all of your sensitive data, particularly the unstructured data that has a tendency to fall between the cracks?
2. Already using USB encryption/Device Control	Encryption is just one part of a comprehensive data protection strategy. How about data leakage via email, web posting, or printing?
3. Don't know where to start	With McAfee DLP, you don't need to know everything up front. McAfee DLP technologies helps you quickly identify which files need to be protected and remediate the relevant files first. This simplifies deployment for you, increases efficiency and saves you valuable time and resources.

Competition/Differentiators

No – Better ◗ Best ●

Category	McAfee	Symantec	RSA	Websense
Capture of non-incident data	●	–	–	–
Forensic Capability	●	–	–	–
Time-to-value Deployment	●	◗	◗	◗
Per-user Virtualization Policy	●	◗	◗	◗
PDF/Image Writer Protection	●	–	–	–
Pre-Built Templates	●	●	◗	◗
Turn-Key Appliance Solution	●	◗	◗	◗
Location & Application Tagging	●	◗	◗	◗
End-user Classification	●	◗	◗	◗

Technology	Differentiators
Time-to-Value Deployment	McAfee Capture Technology provides a historical record of all data leaving the enterprise, helping organizations build better DLP policies faster and more accurately.
Simplified Policy Management	McAfee Data Classification Technology supports rapid inventory, categorization, and automated remediation for large amounts of data on servers and file shares, helping organizations maximize their time and resources by focusing on relevant files.
Unique, Forensic Investigation	McAfee is the only DLP vendor that conducts forensic analysis on data-loss events that occurred prior to the creation of rules – which helps organizations employ more effective and comprehensive DLP policies.

DLP SKUs

- McAfee Total Protection for DLP
- McAfee DLP Endpoint
- McAfee Device Control
- McAfee DLP Monitor
- McAfee DLP Prevent
- McAfee DLP Discovery
- McAfee DLP Manager