Data Sheet

McAfee DLP Monitor

Safeguard vital data

Key Advantages

Identify and protect sensitive information

- Quickly identify sensitive information through an intuitive search engine.
- Conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats.
- Instantly create rules to prevent future behavior.

Capture and index all network traffic

- Filter and control sensitive information to identify hidden or unknown risks.
- Index all types of content and then query and mine it to understand your sensitive data and where it is being sent.
- Monitor internal file share access.

Create and tune sophisticated rules

- Identify more than 300 unique content types over any port and any application.
- Classify network traffic independent of port.
- Scale to support hundreds of thousands of concurrent connections.

Protecting customer and employee personal privacy data—Social Security numbers, credit card numbers, or other personal information—is on everyone's mind today. Accidental disclosure of data due to employee error, lost laptops, and misplaced USB devices are security challenges for nearly every organization. To compound matters, data can be leaked or end up in the wrong hands when it's transmitted and shared through web applications like Google Gmail, Yahoo! Mail, instant messaging, and Facebook. McAfee® Data Loss Prevention (DLP) Monitor is a high-performance data loss prevention solution that can analyze all Internet communications and determine if information is going where it shouldn't. It helps you minimize the workload for your security team, meet compliance requirements, and property intellectual property protection and other vital assets.

Monitor, Track, and Report on Data in Motion

No matter what your business, you need the visibility to identify sensitive information over any application, any protocol, any port, and in any form—with a high degree of accuracy.

With McAfee DLP Monitor, you can gather, track, and report on the data in motion across your entire network—in real time—to find what and how information travels between your users and other organizations. A high-performance, purpose-built appliance that uniquely detects more than 300 content types traversing any port or protocol, McAfee DLP Monitor can help you uncover threats to your data and take action to protect your organization against data loss. In addition, through end-user notification, McAfee DLP Monitor can educate your users on data loss violations to change behaviors without effort.

Scan and Analyze Information in Real Time

Integrated into the network using a SPAN or tap port, McAfee DLP Monitor performs real-time scanning and analysis of network traffic. With more than 150 pre-built rules, ranging from compliance to acceptable use to intellectual property, McAfee DLP Monitor matches entire and partial documents—including fine-grained plagiarism—to its comprehensive set of rules. This enables you to detect anomalies in network traffic, no matter how large or small.

Discover Risks Not Previously Considered

Through detailed classification, indexing, and storage of all network traffic—not just information that matches its real-time rules—McAfee DLP Monitor allows you to quickly leverage historical information to understand what data is sensitive, how it is being used, who is using it, and where it is going. Additionally, you can perform granular investigation and historical inspection of information to detect risk events and data exposure that may not have been previously considered. And when deployed in conjunction with McAfee DLP Discover, you can also identify where data is stored on your network and who owns it.

View Incident Reports to Inform Action

Once traffic is scanned, analyzed, and classified by its classification engine, McAfee DLP Monitor stores all the pertinent information in a proprietary database. Using an intuitive search interface, you can view comprehensive reports of your information, who is sending it, where it is going, and how it is being sent—so you can determine what, where, and how information is leaking. With this knowledge, you can take action to address these threats by applying a range of actions to ensure compliance with regulations and protect sensitive data.

Specifications

System throughput

- Classify content at up to 200 Mbps, without sampling.

Network integration

- Integrates passively into the network using either a SPAN port or a physically inline network tap (optional).

Content types

Supports file classification of more than 300 content types, including:

- Office documents
- Multimedia files
- P2P
- Source code
- Design files
- Archives
- Encrypted files

Protocols supported

- Supports all transmissions over any protocol or port utilizing TCP as a transport protocol.
- Includes protocol handlers for HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more.

Built-in policies

- Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.
- Enables complete customization of rules to meet business-specific needs by leveraging the McAfee capture database.

Complex Data Classification

McAfee DLP Monitor empowers your organization to scan all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property. By combining these object-classification mechanisms, McAfee DLP Monitor builds a highly accurate, detailed classification engine that filters sensitive information and performs searches that identify hidden or unknown risks.

Object classification mechanisms include:

- *Multilayer classification*—Covers both contextual information and content in a hierarchical format.
- *Document registration*—Includes biometric signatures of information as it changes.
- *Grammar analysis*—Detects grammar or syntax of anything from text documents to spreadsheets to source code.
- *Statistical analysis*—Tracks how many times a signature, grammar, or biometric match occurred in a particular document or file.
- *File classification*—Identifies content types regardless of the extension applied to the file or compression.

Specifications: McAfee DLP 5500 Appliance

Component	Description
Processor	2 x Intel E5-2620 6 core, 15 M Cache, 2.0 GHz, 7.20 GT/s Intel QPI
Memory	32 GB DDR3-1333 MHz
Power supply	2 x 760 W hot-swap power supply modules
Hard drives	8x 2 TB SATA 7.2K rpm drives
NIC card	Intel Dual Copper 1 Gbps Ethernet I/O Module
IPMI	Intel Remote Management Modules 4 (AXXRMM4)
Product size	2 rack units (2U)

Specifications: Virtual Machines

McAfee DLP Monitor is available as a virtual appliance that can run on VMware environment. Below are the minimum hardware requirements for running the virtual appliance.

Component	Requirement
Processor	Intel x86 4x vCPU
Memory	16 GB RAM
Hard disk drive(s)	Drive 1: Minimum size, 100 GB for VM software Drive 2: Minimum size, 512 GB for DLP virtual image
Network	4 Virtual NICs
BIOS	Enable VT thread

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60419ds_dlp-monitor_0813_fnl_ETMG