Data Sheet

McAfee Data Loss Prevention (DLP) Manager

Centralize management of McAfee® DLP appliances

Key Advantages

Centralize system management

- Unify policies and rules.
- Streamline incident workflow.
- Deliver comprehensive and flexible reports.
- Configure and manage devices.

Integrate case management and workflow

- Aggregate common incidents.
- Transfer ownership and remediation.
- Restrict users with role-based access and permissions.

Search, mine, and analyze data

- Search historical data quickly.
- Find sensitive data and learn how it is used.
- Tune rules quickly and validate on the fly.
- Perform user investigations.

Filter and group incidents in different ways

- List, group, and summarize incidents.
- Automatically assign incidents.
- Dynamically filter and group incidents.
- Show false-positive workflow.

Organizations today store a tremendous amount of electronic information within their networks. Whether it is sent via email or instant message (IM), stored in a database or file share system, or downloaded to a USB drive to transport to another location, this information is often business critical or otherwise sensitive. Understanding what information exists in the network, whether or not it is sensitive, who is accessing the information, and how is crucial for every organization's security strategy. Losing or compromising this sensitive information is not an option. To reduce the risk of data loss, McAfee DLP Manager helps you determine what information is sensitive and manage its access, storage, transfer, and use from a single, intuitive management console.

End-to-End Data Loss Prevention Management

McAfee Data Loss Prevention (DLP) Manager is designed for large and mid-sized environments that have multiple McAfee DLP appliances deployed throughout the network. With its intuitive, centralized management interface, McAfee DLP Manager provides complete control over these appliances. With McAfee DLP Manager, you have a single view into all McAfee DLP appliances and host agents distributed throughout the network. This enables McAfee DLP learning applications to minimize the time and cost associated with understanding and protecting sensitive data.

McAfee DLP Manager reduces the overall operational expenditure associated with managing and maintaining a security infrastructure by allowing you to accomplish these functions from a central console:

- Manage all policies and rules.
- Access incident and case management workflows.
- Perform searches against one or multiple McAfee DLP appliances.
- Configure and monitor multiple McAfee DLP appliances.

Collaborative Incident Workflow and Case Management

McAfee DLP Manager provides a permissions and workflow framework that encompasses your entire environment and provides role-based access control. Multiple users in the same organization can collaborate on incident workflow and case management.

By enabling cross-discipline involvement, McAfee DLP Manager lets you extend your information protection without increasing the number of people required to support it. It also makes it possible to engage subject matter experts (for instance, legal, human resources, compliance, and content or business owners) in the examination, analysis, and remediation of incidents. Those experts can also help define what data should be protected.

Control of Incident Views Based on Role

With complete role-based access control, you get macro-level risk reporting and statistics as well as micro-level incident information and actions that map directly to organizational responsibilities. You can control these views through role permissions so users see only incidents that are relevant to their job functions. For instance, role-based access control ensures that a compliance user can't perform specific administrative tasks. It also ensures that the same user doesn't see intellectual property incidents or that a content owner doesn't see incidents related to privacy or compliance data.

Centralized Policies and Rules

- Automatically distribute policies and rules to specific or to all McAfee DLP appliances.
- Configure and distribute action rules, including email notification, encryption, blocking, quarantining, redirection, and bouncing.

Incident Workflow

- Centralize the correlation of incidents into a unified incident dashboard.
- Escalate incidents through an embedded case management tool.
- Delegate responsibility for a specific case among key users.
- Use a false-positive workflow to eliminate false positives.
- Automatically update rules affected by workflow changes.

Case Management

- Consolidate and address group-related incidents that require remediation and involve the same stakeholders.
- Implement flexible incident and case logic: multiple incidents can belong to a case, or a single incident can belong to multiple cases.
- Escalate incidents to different teams.
- Access a case history audit trail, including notes.
- Export cases for offline viewing.
- Email case owners a notification if a change is made to a case.

Reports and Incidents

- Access a centralized view of all incidents that have been generated by any McAfee DLP appliance or McAfee DLP Endpoint agent anywhere in the network.
- Generate reports that cover one, several, or all McAfee DLP appliances.
- Automate reporting with 50 packaged reports, each configurable and scheduled for automatic email delivery in PDF and CSV formats.

Dynamic Filters

- Quickly filter information to get to the specific data view.
- Automatically populate filters by clicking the contents of a cell within a table view.
- Dynamically add, remove, and compound filters.

Pre-Configured Roles

- Expedite setup using pre-configured roles for key members of teams within the organization, including administrators, legal, human resources, compliance, operations, and information security.
- Define additional roles with a few mouse clicks.
- Assign permissions to a role in a granular manner.
- Integrate with LDAP or Microsoft Active Directory for centralized authentication services.

Centralized Device Management

- Configure and manage McAfee DLP appliances from a single interface.
- Check the status of any managed McAfee DLP appliance, including CPU utilization, disk utilization, and network throughput.
- View any remediation alarms and alerts that are generated by any managed McAfee DLP appliance.

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 Discover 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	8 GB RAM
Hard disk drive	Minimum size, 1 TB
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

60418ds_dlp-manager_0813_fnl_ETMG