McAfee Data Loss Prevention Discover

Locate, classify, and protect your sensitive data wherever it lives.

Key Advantages

Identification of data leakage risks

- Scan information stored on-prem or in the Cloud.
- Identify where sensitive data is stored and who the content owner is.
- Search and view all scanned data from an intuitive interface.

Policies and customized reports

- Perform queries and then transfer results to a protection rule.
- Use prebuilt compliance, corporate governance, and intellectual property policies.
- Register sensitive information to adjacent information security systems.

Classification, analysis, and remediation of data leaks

- Filter and control sensitive information with multivector classification.
- Index all content and then query and mine it to understand your sensitive data.
- Register and generate signatures to protect documents and the information contained within—even if plagiarized or transposed.
- Send an alert notification if content violates protection policies.

Sensitive information that resides on laptops, shared file servers, and in Cloud storage may be putting your organization at risk. Huge volumes of information—terabytes and even petabytes—must be protected. This is especially difficult because sensitive information isn't always properly labeled. Additionally, in most organizations, there is no way to know or verify whether sensitive data may be at risk or to know where it has proliferated—even with access controls in place. Making matters more complicated, sensitive data typically consists of unstructured data types such as intellectual property (IP) assets that are harder to define than structured data like credit card or Social Security numbers. McAfee® Data Loss Prevention (DLP) Discover helps you locate and classify your sensitive data, find out how it is being used, and protects it against theft or leakage.

What's New in McAfee DLP Discover?

McAfee DLP Discover can now scan and protect data residing in Cloud storage—Box. Policies can be easily defined in McAfee ePolicy Orchestrator® (McAfee ePO™) centralized management software; and scans can be automated and scheduled ahead of time. Special reporting on incidents and detailed analytics are available.

Feature highlights:

- Software-only McAfee DLP Discover offers additional cost saving—hardware or VM-based appliance no longer required.
- Fully deployable and manageable by McAfee ePO software. Share the same management extension and DLP policy as DLP Endpoint.
- Fully aligned with DLP Endpoint classification capabilities.
- Compatible with Windows 2008 and Windows 2012 Servers.
- Supports distributed deployments that leverage idle capacity on existing servers and may be deployed over a wide geographical area.
- Compatible license for DLP Discover appliance versions 9.3.x or DLP Discover software-only version 9.4.

intel Security

Specifications

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

- "Box" Cloud storage
- Microsoft Office documents
- Multimedia files
- Source code
- Design files
- Archives
- Encrypted files
- Built-in policies
- Intellectual property

Repositories supported

- Common Internet file system/server message block (CIFS)[1]
- Network file system (NFS)
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- Databases: Microsoft SQL, Oracle, DB2, MySQL Enterprise

Document Registration

Documents can be registered from any repository. Signatures from registered documents can be used locally for detecting proliferation of sensitive material, or be made available to other McAfee DLP Appliances.

Reporting

The powerful analytics engine for incident and search result views allows you to customize summary views based on any two contextual pivot points. List and detail views, as well as summary views with trending, are available. More than 20 customizable prebuilt and customizable reports are provided with the system.

Preventing Loss of Sensitive Data

From source code to trade secrets to strategic business plans, IP and other information assets are critical to your brand, public reputation, and competitive edge. Protecting data during transmission is critical, but securing sensitive data before it is inappropriately accessed or moved and understanding where it resides should be your first line of defense.

McAfee DLP Discover helps you protect your organization against data loss. Unlike legacy solutions that expect you to know exactly what content you want to protect, McAfee DLP Discover provides comprehensive coverage for obvious information and helps you find the non-obvious.

Determining What Information to Protect

To identify information and proliferation risks, McAfee DLP Discover can be configured to scan specific repositories and identify data for explicit protection. Additionally, all data crawled by McAfee DLP Discover is indexed and made accessible through an intuitive interface, allowing you to quickly search for data that may be sensitive in order to understand who owns the content and where it is stored.

Defining Policies for Protection

Once you know what information to protect, McAfee DLP Discover can help you accurately protect that information. McAfee DLP Discover provides intuitive and unified policy creation, reporting, and management to give you more control over your information protection strategy for data at rest. Key benefits of the policies, rules, and classifications in McAfee DLP Discover include:

- Numerous built-in policies for a simple out-of-box experience.
- Powerful rule-construction engine, from simple structured data (credit cards, Social Security numbers) to complex information (intellectual property).
- Simplified rule creation and validation by transferring search result analysis to a protection rule.
- Integration with adjacent information security vectors to ensure consistent protection.
- Exclusion of public documents and common text to prevent benign information from generating incidents.

Scanning Your Network for Violations

After policies are defined, McAfee DLP Discover can be instructed to routinely scan network resources for policy violations. Flexible scheduling options are available to perform continuous, daily, weekly, or monthly scans.

McAfee DLP Discover automatically scans all accessible resources, including laptops, desktops, servers, document repositories, portals, and file transfer locations for policy violations. You can define scan groups based on IP addresses, subnets, ranges, or network paths. You can also focus scan operations based on specific parameters, such as scanning only My Documents for all users and not system folders, or looking for files owned by specific users or of a certain type or size.

Reviewing and Remediating Violations

McAfee DLP Discover eliminates or minimizes proliferation of sensitive material through integrated incident workflow and case management. If McAfee DLP Discover finds content that violates protection policies, it generates incidents and sends notifications. Incidents created by McAfee DLP Discover can be added to the case management framework, which allows you to involve specialists from numerous organizations within the company to take action on the violation. Additionally, risk dashboards provide easy ways for security personnel to see the profile of policy violations and generate reports based on any data-at-rest parameter of interest.

Specifications: Software-Only

McAfee DLP Discover is available as a software version. Below are the minimum system requirements.

Hardware requirements

- CPU: Intel Core 2 64-bit
- RAM: 4 GB minimum
- Disk space: 100 GB minimum

Supported Platforms

- Windows Server 2008 R2 Standard, 64-bit
- Windows Server 2012 Standard, 64-bit
- Windows Server 2012 R2 Standard, 64-bit

Supported Virtualization Systems

- vSphere ESXi 5.0 Update 2
- vCenter Server 5.0 Update 2

McAfee ePO software and agents

- McAfee ePO 4.6.8 or later; and 5.1 or later
- McAfee agent 4.8.2 or later; and 5.0 or later

Capturing and Analyzing Stored Data

In addition to scanning network resources to detect policy violations, McAfee DLP Discover also indexes all content found at rest in the network and provides you with the ability to query and mine this information to understand your sensitive data. McAfee DLP Discover lets you quickly understand your sensitive data, how it is used, who owns it, where it is stored, and where it has proliferated.

Classify Complex Data

McAfee DLP Discover empowers your organization to protect all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property. By combining the inputs from these object-classification mechanisms, McAfee DLP Discover is able to build a highly accurate, multivector classification, which is used to filter and control sensitive information and to perform 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

McAfee DLP Discover is available as a physical or virtual appliance. Below are appliance specifications.

Component	Description
Processor	2 x Intel E5-2620 6 core, 15 MB 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	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

1. McAfee DLP Discover 9.4 Software-only version currently supports CIFS, Microsoft SharePoint 2010, and Microsoft SharePoint 2013.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com