



# Introduction

**Today's security professionals face a daunting challenge: Protecting the organization's most valuable asset, its information.** As organizations invest in new business systems and processes to exchange critical information in real-time, security teams struggle to identify which information needs protection and more opportunity exists for information leaks. Most Data Loss Prevention (DLP) solutions today provide a means of protecting sensitive information based on pre-configured policy templates and easy-to-use policy wizards, but the problem with today's DLP solutions is that they fundamentally expect you to "know" exactly what needs to be protected and from whom to protect it. McAfee has taken a unique approach to data loss prevention; starting with the premise that data protection should not require security teams to know exactly what information needs protection from whom but that the technology should be able **to learn and adapt to the changing needs of the business uncovering not just what you know, but what you don't know.**

## The Challenge with Today's DLP Solutions

The challenge with today's DLP solutions is that they fundamentally expect you to "know" exactly what needs to be protected. In the case of "obvious" data—such as Social Security Numbers and Credit Card Numbers—this is relatively easy, as the data is represented in a semi-structured and obvious form.

When dealing with more complex data with numerous intricacies—such as intellectual property—the data is difficult to "describe" using simple expressions and keywords. To compound the problem, security teams are expected to know "how" this "unknown" data should be protected. Not only must the security team first figure out what the data is, but then they must also figure out where it should be stored, who should be accessing it, where it should be allowed to go, and how.

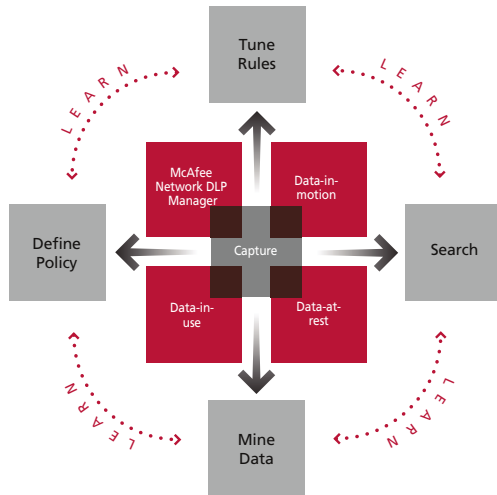
This chasm that exists between the capabilities of the DLP solution and the fundamental understanding of each business unit's intellectual property AND the business process surrounding it is the single greatest challenge threatening the value of DLP in the enterprise today. McAfee Network Data Loss Prevention (DLP) adaptive data protection overcomes these challenges and empowers

you to quickly—and accurately—protect your known and unknown sensitive data.

## What are McAfee Network DLP Learning Applications?

McAfee understands this issue very clearly and provides a series of capabilities that address the problem directly. McAfee Network DLP doesn't expect you to "know" exactly what information is sensitive and the business process surrounding it. Rather, McAfee Network DLP helps you "learn" what this data is and how it is being used in your environment today.

This capability, unique to McAfee Network DLP, is enabled by how McAfee Network DLP captures and indexes all content—regardless of whether or not a rule was violated—which is then made available to the user through an intuitive search interface. This capture database, which is the cornerstone of McAfee Network DLP learning applications, are designed to help you better understand your sensitive data, who is using it, how it is being used, where it is stored, and where it is going in your environment. With McAfee Network DLP learning applications, the process of identifying—and protecting—your sensitive data is reduced from months to days.



*McAfee Network DLP helps organizations protect obvious information as well as the not-so-obvious information, including intellectual property and complex information structures.*

### How do McAfee Network DLP Learning Applications Work?

Today's DLP solutions simply evaluate content to identify rule violations, take action, and then log the violation along with the object in question. In this way, today's DLP

solutions provide little to no value regarding the rest of the data that was identified that did not violate a rule. In this way, the DLP systems of today only provide value based on the rules that are configured on the system. McAfee has taken a different approach. With McAfee Network DLP, all content that is identified in motion on the network or at rest on the network is evaluated for policy violations—like other DLP systems. McAfee Network DLP is different in that all content—and the context associated with each—is indexed for later use, and stored in the McAfee capture database. This index and stored content is then made accessible through an intuitive search interface, allowing you to perform simple or complex queries to learn more about your data. Let's use an example to illustrate.

Assume a legacy DLP solution is deployed to identify any credit card numbers (CCNs) found in motion unencrypted on the network. As CCNs pass by the device, an incident is generated and you the administrator are notified that a CCN was about to pass by unencrypted. An email can even be sent to let the sender know that the data should have been sent in an encrypted manner. This gives you the visibility necessary to approach the system administrator—or user—to let them know about the fact that CCNs must be transmitted in an encrypted manner to ensure PCI compliance. Now let's take the example a step further.

Details	Content	Sender	Recipients	Subject
[icon]	[icon]	yigrah.gigrah@netvision.net	DB Lark (gpatman@yahoo.com)	send me message - confidential
[icon]	[icon]	gpatman1 (gpatman1@netvision.net)	gpatman1@yahoo.com	mail attach - loss of money
[icon]	[icon]	Karl Boje (karlboje@ga-llc.com)	Karl Boje (karlboje@yahoo.com)	Confidential
[icon]	[icon]	Karl Boje (karlboje@ga-llc.com)	Karl Boje (karlboje@yahoo.com)	Confidential
[icon]	[icon]	Karl Boje (karlboje@ga-llc.com)	Karl Boje (karlboje@yahoo.com)	Confidential
[icon]	[icon]	Unknown	gpatman1@yahoo.com	Confidential information
[icon]	[icon]	Unknown	gpatman1@yahoo.com	Messaging System
[icon]	[icon]	Unknown	gpatman1@yahoo.com	Confidential information

Sender	RecipientDomain	hits
Unknown	Total	10
	yahoo.com	7
	netvision.net	2
Karl Boje (karlboje@ga-llc.com)	Total	3
	yahoo.com	3
yigrah.gigrah@netvision.net	Total	1
	yahoo.com	1
gpatman1 (gpatman1@netvision.net)	Total	1
	yahoo.com	1

*From a simple search, you can quickly identify sensitive data that you didn't already have a rule for—and see who has been emailing it out of the company, and where they have sent it to. With analytics views, you can pivot incident and search data on any parameter to better understand behavior—and unknown business processes.*

## Learning Applications to Identify Sensitive Data and Business Process

Assume now that you are charged with protecting documents that contain product strategy details for the next three years, as it has recently been determined that there was data leakage in the last week involving such information. With a legacy DLP solution, you are not given visibility into what happened, because you didn't have a rule pre-configured to look for documents that contain this information. With McAfee Network DLP you can use the intuitive search interface—the gateway to McAfee Network DLP learning applications—to search for documents containing terms and expressions contained within the document—even though you didn't already have a rule configured. Within seconds, McAfee Network DLP presents you with:

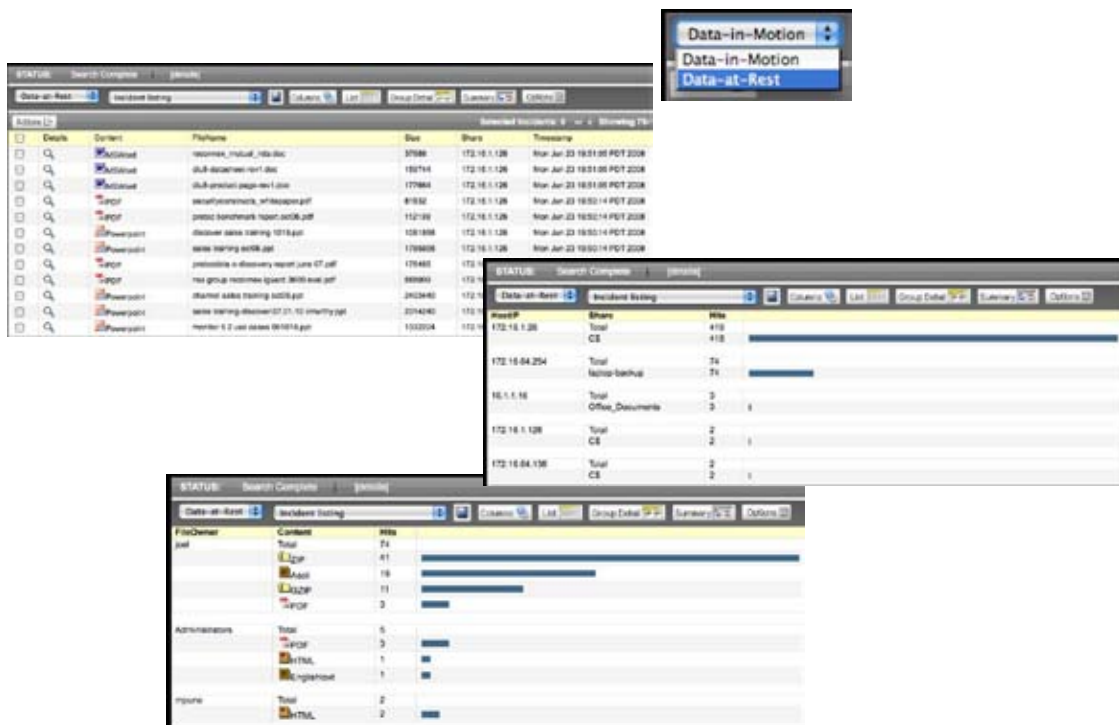
- A view of all documents over any protocol containing the keyword 'confidential'.
- Visibility into who was sending these documents out of the company.
- Visibility into where these documents were going by recipient or domain.
- A view into what hosts and shares on the network where these files are stored.

- Understanding of who owns files that are at rest on the network that contain keyword 'confidential'.

With McAfee Network DLP, you have complete visibility into historical information—not only for the purposes of investigating past data leaks in situations where you didn't have rules already configured, but also to minimize the amount of time necessary to get up to speed on how these product strategy documents are being used today and how it should be protected.

### Save time and money with McAfee Network DLP

With legacy DLP solutions, you would still need to have a series of meetings with content owners to determine what product strategy documents are, who should be using them, where they should be sent out of the company, how they should be sent, where they should be stored on the network, and so on. With McAfee Network DLP, you save time—and money—because this information is already readily available to you. Rather than requiring a series of laborious meetings, you can start with the data you already have and tighten from there—saving you days, weeks, and even months of time. The time you save also turns into faster time to protecting your sensitive data.



Additionally, simple searches can be performed to identify sensitive data at rest that you didn't already have a rule for—and see where it is stored on the network, on which machines, on which shares, and who owns the data—to apply protection proactively.

## Learning Applications to Minimize Time Spent Creating and Tuning Rule

McAfee Network DLP learning applications aren't only about understanding historical data to identify past data leaks or minimize time spent creating rules. McAfee Network DLP learning applications also help you make sure your rules are air tight in a matter of time that is infinitely shorter than what today's legacy DLP solutions can provide you. With McAfee Network DLP, you can perform a search over historical information using a rule that is already running on the system. Search results can then be examined to see how the rule behaved using historical data, and the search query can be adjusted so you end up with a result set that is accurate.

Similarly, you can start with a simple search over historical information to find sensitive data going to unapproved recipients or stored in unapproved locations. In a matter of seconds Reconnex presents you results from simple queries that you specify to help identify this sensitive data and how it is being used. Adjustments can be made to the search to help focus your results on a specific set of instances that may be of concern. After you have iterated through the search to identify instances where this sensitive data is or has been compromised, you can simply click a button to transfer the search query into the construction of a new rule. Learning applications help simplify the process of tuning existing rules and created new rules—while providing the accuracy you demand. Let's look at another example.

With today's legacy DLP products, in the scenario above you wouldn't have visibility to the past data leak. Additionally, it would take days upon weeks—even months—to work with all of the content owners to identify what confidential data is and how it required protection. That time between problem identification and rule deployment is time where your data is not protected. Now, let's assume your 'confidential' rule is producing false positives. It turns out that Joe in product development is allowed to send confidential documents out to specific business partners in Asia that are part of a contract manufacturing facility. With today's DLP systems, you have to manually add each exception to the rule as the false positives come into the system. This is a time-consuming, laborious, iterative process.

With McAfee Network DLP you can simply test your rule against historical data using McAfee Network DLP learning applications. This will allow you to immediately see all instances where 'confidential' is leaving the company—along with who is sending it, where it is going, and how.

You can take this information and have the content owner approve or disapprove every single recipient or every single domain, and get the changes out of the way quickly. Once you update the rule, you can yet again test it using McAfee Network DLP learning applications to validate that the rule is accurate. In a matter of minutes, rules deployed on McAfee Network DLP can be tightened to near-perfect accuracy—a process that can take days and weeks—even months—with legacy systems.

## Learning Applications to Improve Investigations

To take the same example further, assume that you identified a potential data leak. This leak involved a particular employee who seems disgruntled after discussion with their management. The management team and content owners are concerned about what other activity this employee has been engaging in up to this point. With legacy DLP solutions, you are given complete visibility into every- thing that the employee has done that has violated configured rules. Any other activity that did not violate a rule is not recorded and thus not made available to you. With McAfee Network DLP, all content in motion and at rest is indexed whether a rule was violated or not. Through McAfee Network DLP learning applications, a simple query through the intuitive search interface returns information about all network flows associated with that particular user, including email, webmail, instant messenger, file transfers, and more. Additionally, content identified through crawling the user's laptop and files owned by that particular user are available at your fingertips.

With McAfee Network DLP, learning applications allow you levels of visibility not provided by today's legacy DLP solutions, which helps you not only better understand your sensitive data and how it should be protected, but also perform investigations— even for things that didn't violate a system rule.

## Conclusion

Only McAfee Network DLP provides learning applications to help eliminate the key information security challenges facing your organization with deploying DLP technologies. By indexing all content in motion and at rest, and making this information available through a simple and intuitive search interface, McAfee Network DLP allows you to quickly identify your sensitive data, who is using it, where it is being sent, and where it is stored, and investigate activity—whether a rule was configured or not. McAfee Network DLP doesn't expect you to "know" exactly what needs to be protected—or how. Nor does McAfee Network DLP expect

you to “know” where your critical information is vulnerable and who or what your threats may be. Rather, McAfee Network DLP learning applications help you “learn” about your sensitive data, your business process, and gain better insight into risk.

For more information about McAfee Network DLP solutions (formerly Reconnex) please visit: [www.reconnex.net](http://www.reconnex.net) or call us at 888.847.8766—24 hours a day, seven days a week.

For more information about all of McAfee’s Data Protection solutions please visit: [www.mcafee.com](http://www.mcafee.com) or call us at 888.847.8766—24 hours a day, seven days a week.

## About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world.

With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security. [www.mcafee.com](http://www.mcafee.com)

---

McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved.

5025\_br\_f\_dlp\_network-adaptive-protection\_1008