



**Close the Data Loss  
Prevention Coverage Gap**  
Neutralize the insider threat

## **Table of Contents**

<b>Executive Summary</b>	<b>3</b>
<b>The Insider Data Loss Problem</b>	<b>3</b>
<b>So Far, Not So Good</b>	<b>4</b>
<b>Demand More from DLP Products</b>	<b>4</b>
<b>The McAfee Solution</b>	<b>5</b>
<b>Universal Protection</b>	<b>5</b>
<b>A New Model: Content-Aware Control</b>	<b>6</b>
<b>Safeguard Unmanaged Systems</b>	<b>6</b>
<b>Constant Control, Even “On the Go”</b>	<b>7</b>
<b>Verifiable Enforcement</b>	<b>7</b>
<b>Monitor for Insight and Accuracy</b>	<b>7</b>
<b>Convenient Compliance and Administrative Reporting</b>	<b>7</b>
<b>The McAfee Advantage</b>	<b>7</b>
<b>Long-Term Risk Management</b>	<b>7</b>
<b>Neutralize the Insider Threat</b>	<b>8</b>

# Neutralize the insider threat

## Executive Summary

**On December 13, 2006, the Privacy Rights Clearinghouse announced the dismal milestone of 100 million records breached since the ChoicePoint data loss incident ignited a public furor in February 2005. Despite years of regulatory pressure, data loss prevention remains a challenge for organizations of all sizes.**

Regardless of whether data loss happens accidentally or as a result of malicious activity, the effect on the organization can be severe: loss of trade secrets, loss of customer goodwill, and regulatory penalties. To stem the damage to balance sheets, brands, and competitive advantage, organizations must adopt a new approach to protecting customer data and intellectual property assets.

Why are current protections insufficient? No data loss coverage. Driven by industry regulations and internal governance policies, most security programs still concentrate on limiting unauthorized access. They fend off external attacks with traditional data security measures including firewalls, intrusion prevention, and anti-spyware. They rely heavily on identity and access controls and, in some cases, data encryption to limit exposure of sensitive information. But these approaches leave coverage gaps that enable an insider threat: inadvertent and deliberate loss by authorized users.

*According to the 2006 CSI/FBI Computer Crime and Security Survey, a remarkable 68 percent of survey respondents had experienced tangible losses attributed to insiders.*

A new data loss prevention solution from McAfee® closes this gap. It combines host and network protections throughout the data usage lifecycle, from creation and manipulation to transfer and transmission. Organizations gain consistent, reliable data loss prevention across applications, network channels, and even physical devices.

The McAfee Data Loss Prevention (DLP) solution makes it possible for organizations to enforce policies and monitor and report on improper usage—even when laptops are physically disconnected from the network. It helps inform users of proper policies while preventing losses. It also offers new visibility into actual data handling to help security managers appropriately direct investments in safeguards, training, and process improvement. Because this protection comes from McAfee, it complements and reinforces other network and host-based defenses. The McAfee DLP solution closes the authorized-user coverage gap and provides an easily managed, must-have element of any security risk management program.

## The Insider Data Loss Problem

In a typical month, data loss incidents make mainstream news more often than violations of the Sarbanes-Oxley Act (SOX). While hacking gets justified attention, a great number of losses are due to authorized users inside the organizations. The 2006 CSI/FBI Computer Crime and Security Survey indicated a remarkable 68 percent of firms surveyed had experienced tangible losses attributed to insiders. These losses tarnish reputations and brands, jeopardize competitive advantage, and require costly remediation. Consider the fourth quarter of 2006. According to the Privacy Rights Clearinghouse and other public sources, insider-enabled data losses ran the industry gamut from health care to government to financial institutions:

- Hertz Global Holdings said it had dropped Deutsche Bank from its underwriting team after “several emails” discussing its imminent \$1.5 billion initial public offering were inadvertently sent by the bank to about 175 institutional clients
- Industrial espionage charges were filed against a Chinese-Canadian engineer for theft of military training software
- The Republican National Committee inadvertently emailed a list of donors’ names, Social Security numbers (SSNs), and races to a New York Sun reporter
- A Cal State, Los Angeles, employee’s Universal Serial Bus (USB) flash drive was inside a purse stolen from a car trunk. It contained personal information on more than 2,500 students and applicants of a teacher credentialing program

- A Gundersen Lutheran Medical Center employee in Lacrosse, Wisconsin, was convicted of using patients' personal information to apply for credit cards
- Bank of America announced a former contractor had stolen personally identifiable information (PII) of an undisclosed number of customers (Charleston, South Carolina)
- The Bowling Green, Kentucky, police department accidentally published a report on its web site containing driver's license numbers and SSNs
- A printout of 21,000 student records disappeared at Nassau Community College in Garden City, New York
- Names and SSNs of "several hundred" health care providers were mistakenly posted online by Segal Group, a contractor hired by the state of Vermont

What do these losses have in common? Authorized users. Users already inside the organization had a business need to view and handle sensitive information. Through uninformed misuse, errors in judgment, or malicious intent, their legitimate access to information led to losses that caused financial and legal liability, and public relations headaches.

Are these losses new? In some cases, yes, as more business and government practices go online to support distributed, just-in-time operations. In other cases, they are simply visible now. Privacy regulations like California Senate Bill 1386, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the European Union Data Privacy Directive now force public notification of breaches of PII.

## So Far, Not So Good

The traditional approach to data security emphasizes "keeping the bad guys out" using firewalls, intrusion prevention, anti-spyware, and data encryption products.

To control unauthorized information usage by insiders, many companies deploy identity management systems and use access control lists. These traditional security and access controls are helpful, but they don't fully protect companies from data loss.

Training and education help, but the same 2006 CSI/FBI Survey indicated that most respondents feel their companies are not investing enough in security awareness.

In recent years, security vendors have created a new class of products known as data loss prevention (DLP) solutions. Most of these first-generation DLP solutions operate at the gateway to prevent unauthorized transfer of sensitive data through email and the web.

But these gateway solutions don't control actions on the desktop.

*In February 2006, Gartner Content Monitoring and Filtering Research indicated that the market would likely evolve to the "successful blocking of all channels on the network and hosts from which data can be stolen. This would include host-based agents that can stop someone from downloading sensitive data—for example, through a Universal Serial Bus (USB) drive—and printing it and walking out the door."*

—Paul E. Proctor and Rich Mogull, 23 February 2006, Gartner ID Number G00137664

## Demand More from DLP Products

Of the data loss incidents mentioned above, only the email gaffe by Deutsche Bank might have been prevented by the current generation of gateway-based DLP products. To consistently prevent all of these types of data losses, organizations need to monitor content across its lifecycle.

Sensitive data is often stored on centralized servers, but it's also created, altered, printed, and copied by authorized users. It is shared—in hard copy, on USB drives, and over networks. When they are finished, users archive it—on a local hard drive, by transfer to CD-ROM or USB drive, in printed files, or by transmitting it over the network. Full protection requires consideration of these legitimate uses and needs and awareness of organizational boundaries—like the finance domain, the marketing intranet, and the public web site. The right approach allows appropriate business use and timely sharing of information within and outside of the organization.

The hallmarks of this new standard of DLP should include:

- Universal protection of data across network channels, applications, and physical devices (USB drives, printers, or fax machines)
- Granular, content-aware control that allows appropriate actions and lets normal business flow
- Unmanaged systems protection to block content distribution by in-network and guest endpoints (for example, printers, mobile devices, or contractor laptops)
- "Protection on the go" to control data usage and transfer even when laptops are disconnected
- Verifiable enforcement of regulatory and governance policies

These enhancements would help with insider data losses:

Necessary Prevention	Data Loss Channel	Typical Loss Incidents
Attempts to copy and paste privileged information should be flagged and blocked	Cross-application copy/paste	Bowling Green Police Department
Prevent publishing of sensitive information to external web sites	Web posting	Segal Group/State of Vermont
Block printing of sensitive information except to physically controlled and managed printers	Uncontrolled network printing	Nassau Community College
Prohibit copying of information at endpoints (USB devices or CD-ROMs)	Transfer of data to portable storage devices	Cal State, Los Angeles; industrial espionage
Block copying of information when users are disconnected	Transfer of data while offsite	Bank of America
Block distribution of sensitive information outside internal networks, including through personal email	Email disclosure of confidential business plans and sensitive information	Hertz Global Holdings
Control transmissions by unmanaged endpoints, such as mobile devices and guest laptops	Email disclosure of confidential business plans and sensitive information	Republican National Committee

**Table 1: New protections should improve coverage across the many channels authorized personnel use to conduct legitimate business.**

Since compliance and governance requirements seem to only expand, these capabilities need to enable management by feeding usage and violation information into risk management and reporting systems. The goal: a coherent, unified overview that will save time and reduce the likelihood of gaps and mistakes when auditors come calling.

### The McAfee Solution

For decades, McAfee has worked directly with customers in security conscious and heavily regulated industries to implement strong, effective data protection. As part of its vision of proactive security risk management, McAfee has taken a leadership role in DLP. McAfee has created the first comprehensive DLP solution that combines the efficiency of network operations with the granularity of endpoint controls, all under a single management umbrella.

### Universal Protection

The McAfee DLP solution combines the strength of host and network protections with centralized management to drive consistent, comprehensive coverage throughout the usage lifecycle. To achieve this high degree of protection, it controls the insider threat from two different vantage points: the end user or endpoint and the gateway or network. It oversees data as it is accessed, created, and manipulated at endpoints to block inappropriate actions. It safeguards data being transmitted across network boundaries to prevent deliberate or inadvertent transfer. By integrating both host and network protections, the McAfee DLP solution delivers complete, reliable, and verifiable coverage.

*With 350 communications networks located in 163 countries, an IT team at one McAfee DLP customer secures data that crosses the globe. It is a critical objective of this team to ensure that private information, such as who makes a call, when, and where, is protected. This telecom customer places an equally high importance on securing data on 4,000 internal personal computers, 20 percent of which are laptops that require “protection on the go.”*

McAfee DLP Host monitors and controls the usage of data at the endpoint. By itself, McAfee DLP Host offers superior protection to anything available previously. Universal protection, even for USB drives and laptops on the go, increases oversight and confidence about endpoint activities. Content-aware control improves the accuracy of policy implementation to prevent losses while allowing appropriate business activities.

McAfee DLP Gateway complements this host protection with extra transmission control at the perimeter. It ensures that all computers on the network—including unmanaged devices such as BlackBerry PDAs and non-Windows® computers—are unable to transmit sensitive data through network channels

These two protections work together to implement usage policies that constrain inappropriate use by both authorized and unauthorized users. An extensible management console, the McAfee ePolicy Orchestrator®, simplifies monitoring, policy enforcement, audit, and reporting.

Data Loss Channels	McAfee Hybrid DLP Solution— Most Comprehensive Coverage		
	Corporate Network	Public Internet	Disconnected
Email	✓	✓	✓
IM	✓	✓	✓
HTTP, FTP	✓	✓	✓
Copy and paste	✓	✓	✓
Local/screen capture	✓	✓	✓
External (USB)	✓	✓	✓
Web mail	✓	✓	✓
Agentless devices	✓		
BlackBerry	✓		

**Table 2: By combining controls at host and gateway, McAfee can prevent sensitive data transfer or transmission and provide universal coverage for data loss prevention.**

If a user tries to copy sensitive information such as customer lists out of one application and into another (for example, from a support or CRM database to email), that action can be blocked. To protect intellectual property like source code or blueprints, McAfee can block specific types of sensitive content being printed, or prevent endpoints from writing to a USB drive or CD-ROM.

The result: universal protection of sensitive content over any transfer or transmission channel.

McAfee DLP does not just prevent the loss; it educates the user to encourage the right behavior. When an inappropriate transfer is attempted, the pop-up error message can include references to policies and educational materials to help users understand and correct their usage. The system can also flag violations if they pass a threshold to identify repeated violators who need additional attention.

## A New Model: Content-Aware Control

Up to this point, data transfer protection has tended to be black and white, off or on. Users could either send or not send information across certain channels, through certain applications, or from certain locations. This high-level blocking has been irritating and disruptive for end users, getting in the way of desirable business operations by limiting appropriate use. Often these constraints drove risky behavior—like using personal email accounts to transfer information—not through malicious intent, but to get the job done.

To overcome this weakness, McAfee DLP uses content-aware technology to monitor and specify the transfer of discrete confidential data regardless of format or usage. Rather than restricting classes of actions as a whole, McAfee DLP selectively allows or blocks the action based on

content-specific keywords, text patterns, the classification in the fingerprint (a permanent tagging technique that associates classifications with content in the file), and the network destination. For instance, finance users can be authorized to send profit and loss information to other finance users, but blocked from sending it to all others. In this way, legitimate uses are permitted while inappropriate actions are prevented.

*Legitimate uses are permitted while inappropriate actions are prevented.*

To maintain performance, the content-aware technology efficiently fingerprints only the files in use, rather than every file. With fewer fingerprints to compare, when a file is handled, the system can quickly and accurately determine if a file may be transferred. The check is rapid, and the user and administrator see very few false positives and false negatives—improving confidence in the system.

McAfee DLP recognizes hundreds of different file types and protects the sensitive information regardless of the format in which it is stored or manipulated. McAfee protection is undeterred by compression, encryption, or translation to PDF. Organizations can block copy and paste, screen scraping of data, peer-to-peer transfer, and even sending data in an instant message.

Controls can be imposed on a group, application, or network level to simplify deployment and maintenance. Applications can be managed by type, matching the observation level to the perceived risk while maintaining system performance. To target common mistakes (that amplify damage because they easily go unnoticed), web posting of specific content and transmission to specific network addresses can be blocked.

## Safeguard Unmanaged Systems

McAfee DLP Host protects endpoints under the security manager's control, but what about unmanaged endpoints? Often contractor laptops and personal printers or PDAs pose a coverage gap. To provide universal coverage, McAfee DLP Gateway will protect those endpoints that lack DLP technology, blocking outbound transfer of sensitive content. In addition, McAfee DLP Gateway offers the option to protect against malicious software trying to enter the network, including spam, viruses, Trojans, and spyware. Since spyware is specifically designed to harvest and transmit sensitive information, this dual-blocking approach at the gateway provides both logical and extremely effective protection.

## Constant Control, Even “On the Go”

When a user leaves the organization’s local network, traveling or at home, McAfee DLP remains in control of sensitive data usage. If an offline user attempts to write a sensitive file to a USB drive, a pop-up window flags the error and blocks the action. When the system reconnects, the violation is transmitted to the administrator for tracking.

## Verifiable Enforcement

Information privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), SOX, the Gramm-Leach-Bliley Act (GLBA), and the European Union (EU) Directive are designed to control the transmission of personal information, so email compliance controls should be a top priority for affected organizations.

McAfee DLP includes pre-defined English dictionaries and heuristic rules to scan email messages for a wide variety of non-public, sensitive information including protected health information and personally identifiable information. Should regulated information be detected within the message or over 200 types of file attachments, McAfee DLP can take appropriate action to comply with regulations, including blocking, encryption, quarantine, or rerouting.

## Monitor for Insight and Accuracy

Many companies are eager to boost protection, but not at the expense of productivity. McAfee’s monitoring and analysis tools allow organizations to define effective rules and settings and “test-drive” them in monitor-only mode. Managers can understand their real data usage and transmission problems and validate that policies are appropriate before launching live deployments.

The policy analyzer assists quality control by ensuring that rules and tags match up for complete coverage. It can also flag inactive or disabled rules that might weaken protections or highlight an administrative error. These tools help ensure the appropriate level of protections are implemented and maintained, despite changes in data types and rules.

## Convenient Compliance and Administrative Reporting

For most organizations, documentation of policy compliance and organizational improvement represents the most painful everyday hassle imposed by regulatory and governance requirements. To enable daily and periodic oversight and reporting, McAfee DLP helps security officers unobtrusively observe, maintain, and control the level of data security within the organization. The comprehensive reporting engine offers a wide variety of operational,

auditing and executive reports, including special reports needed to comply with government regulations.

To understand usage or a specific event, security managers can see detailed information and filter based on various criteria such as time, date, user and computer name, specific rule, or version. Reports and specific files or violations can enable forensic investigation or be easily preserved as evidence.

Much of the insider threat comes from inadvertent error. McAfee’s detailed analysis and reporting gives organizations the insight to promptly and properly apply education, training, and management resources where they are most beneficial and necessary. The embedded error messages and pop-up notices help users correct their own behaviors. And these notices are flagged to the administrator for follow-up. In the event of inappropriate, incorrect, or just plain onerous policy, adjustments can be recommended and justified with data.

With the McAfee DLP solution, customer and proprietary data can flow within the organization without fear of being published or transmitted inappropriately. The result is uninterrupted business that complies with policy.

## The McAfee Advantage

McAfee’s security experience means convenience and confidence for enterprises and other organizations. The McAfee DLP solution uses trustworthy technology proven in millions of installations. McAfee tests extensively for compatibility and reliability, and demanding customers have demonstrated McAfee’s scalability and sustainability.

McAfee products afford security managers a comprehensive view of their security protection and risk posture using the ePolicy Orchestrator. This unified management console helps make sense of often complex processes. Installation, updates, and status checks are easy with a single view and “one-click” deployment. Managers can readily recognize security events, identify trends, and fulfill tedious reporting requirements. This single console delivers financial benefits by reducing training and management time and speeding remediation.

## Long-Term Risk Management

McAfee is the largest dedicated security company. By concentrating on security risk management, McAfee helps its customers understand their threats and liabilities and take action to maintain or improve business operations. McAfee DLP expands the range of coverage and capabilities that organizations can rely on to protect their brands, sensitive information, and intellectual property. As the DLP market matures and evolves, organizations can count on McAfee to aggressively extend and integrate protections across devices, channels, and safeguards.

## Neutralize the Insider Threat

Every day, more of an organization's assets and competitive edge derive from intellectual property and brand reputation, while more regulations aim at restricting use of PII. Existing security protections are not sufficient to contain the risk of financial damage and legal liability from data loss.

Breaches, either through inadvertent error or deliberate theft, continue through lingering gaps in coverage for authorized users. These users are already inside the organization and have a business need to view and handle sensitive information. But legitimate access to information does not entitle users to remove that information from the enterprise.

*Existing security protections are not sufficient to contain the risk of financial damage and legal liability from data loss.*

With the McAfee DLP combination of endpoint and network protections, organizations can now enforce policies on and identify attempted violations by authorized users. McAfee DLP closes the coverage gap with:

- **Universal protection** of both authorized and unauthorized usage across network channels, applications, and physical devices
- **Content-aware control** that allows appropriate actions to let normal business flow
- **Unmanaged systems protection** to block content distribution by in-network and guest endpoints
- **“Protection on the go”** to control data usage and transfer even when laptops are disconnected
- **Verifiable enforcement** of regulatory and governance policies

To raise your standards for data loss prevention across the usage lifecycle, visit [www.mcafee.com](http://www.mcafee.com) or contact your McAfee sales representative.