

# Trend Micro Data Loss Prevention for Endpoint 5 vs. McAfee Host Data Loss Prevention 3: Endpoint Data Loss Prevention Effectiveness Evaluation

## Executive Summary

Trend Micro, Inc. commissioned Tolly to conduct a comparative analysis of Trend Micro Data Loss Prevention (DLP) for Endpoint versus McAfee Host Data Loss Prevention.

Engineers deployed prototype environments for both solutions focused on providing protection for Windows XP endpoints.

Tests show that the Trend Micro DLP solution provides greater protection for structured and unstructured data, such as documents related to privacy and intellectual property. Furthermore, Trend Micro DLP proved significantly less complex to install and configure than McAfee's solution. Where Trend Micro had built-in support for all applications tested, McAfee required manual configuration for commonly-used applications such as instant messenger and CD/DVD burning. (Note: While the McAfee solution provided pre-configured applications, these did not function without manual configuration.)

Some channels supported by McAfee were only able to detect "tagged" (unstructured) data and, in some cases, could only monitor the channel but not actively block the sensitive data from leaking. McAfee's support for removable devices has a time lag that can allow data to be copied and removed from the system without even being logged to the security log. See Figure 1.

The Trend Micro solution protects more threat vectors than the McAfee offering, is more consistent in its approach, and in our opinion, provides a more effective security perimeter for protecting data in use, at rest and in motion.

## The Bottom Line

The Trend Micro Data Loss Prevention solution:

- 1 Protects more data channels than the McAfee solution and provides more granular controls
- 2 Provides built-in support for a wider range of applications and data protection scenarios
- 3 Provides a more intuitive management console and work flow engine
- 4 Provides pre-configured compliance templates like PCI-DSS, GLBA, US PII, SB-1386 and HIPAA
- 5 Delivers a more secure solution for protecting sensitive data from loss via Windows XP endpoints
- 6 Delivers a better user experience as data protection does not interfere with normal use of applications



## Introduction

Driven by a competitive business environment, often coupled with regulatory mandates, data loss prevention has become a high-priority objective for businesses of all sizes.

There is no industry standard or general practice for deploying DLP and, thus, implementations vary by vendor. Solutions can include agents deployed on desktops and laptops managed by central policy servers and/or devices attached directly to network ports to monitor traffic.

This test focused on an endpoint-based implementation. McAfee also has a network-based DLP (NDLP) offering that can be deployed in conjunction with its agent-based solution. Trend recently released a Network-based DLP compliance module, and plans to launch a fully integrated Network DLP solution in 2010. NDLP was outside the scope of this test.

The test plan evaluated: 1) the capabilities of each offering to define/protect sensitive data, 2) the specific channels protected by offering (i.e, email, Webmail, USB drives, IM, CD/DVD, etc), 3) the level of protection offered when sensitive data was fragmented or otherwise obfuscated and 4) the user experience.

The tests were drawn from Tolly Common Test Plan #1130 Data Loss Prevention. This industry-first, vendor-neutral, test plan is built collaboratively with and open to review by security experts from the vendor and research communities.

## Test Results

### Identifying Protected Data


Both Trend Micro and McAfee provide methods for identifying sensitive data via both dynamic and static means.

Dynamic identification involves using data patterns, keywords and/or file metadata to detect sensitive

**Trend Micro, Inc.**

**Trend DLP for Endpoint 5**

**Endpoint Data Loss Prevention Effectiveness**



*Tested January 2010*

data without the need for a system administrator to have to identify a document (or set of documents) through the administration system.

<b>McAfee Host DLP V3 Solution Limitations Uncovered</b>	
Area	Issue
Installation/ Configuration	Common applications, such as AOL Instant Messenger and CD/DVD burner (Nero Express) require manual configuration.
Channel Coverage	Incomplete support of data types. Some channels can detect only "tagged" (unstructured) data and not data that is dynamically defined by keywords, dictionaries or regular expressions.
Protection	In several instances, channels can only be monitored. Thus, users can be notified that data is lost, but the loss cannot be prevented.
Protection	Removable device support works by deleting the files after they are copied. If users disconnect the removable device immediately, data can be taken without so much as being logged by the management system.
Protection	Incomplete protection of Instant Messenger. Need to configure at least two protection rules to get suboptimal protection.
User Experience	Web post protection interferes with user operation.

Source: Tolly, January 2010 Figure 1

### Systems Under Test

#### Policy/Management Server Software

Vendor	Product	Version	Platform	Notes
McAfee	ePolicy Orchestrator	4.5.0 (Build 753)	Windows Server 2003 R2 (32-bit)	For this test, both McAfee server components were deployed on the same machine.
McAfee	Data Loss Prevention	3.0.0.711	Windows Server 2003 R2 (32-bit)	
Trend Micro	Management Server	DSC-5.0-1301	CentOS Linux Release 4.6 kernel 2.6.9-67	

#### Windows (XP SP2) Agent Software

Vendor	Product	Version	Notes
McAfee	Agent	4.0.0.1421	Pre-requisite for DLP agent
McAfee	Data Loss Prevention Agent	3.0.0.708	
Trend Micro	Trend Micro DLP for Endpoint	5.0.1331	

Note: Several hotfixes/patches were applied to the McAfee components to resolve problems encountered during initial test runs.

Source: Tolly, January 2010

Figure 2

This approach is often used with structured data types.

The vendors take different approaches to identifying unstructured data that is to be protected.

Trend Micro’s approach to identifying unstructured data is termed “fingerprinting” where McAfee calls its approach “tagging”.

With Trend Micro, a system administrator targets particular document repositories to be “fingerprinted” and added to a data store of protected digital assets.

McAfee similarly scans document repositories but “tags” the data as being sensitive. They also allow administrators to define that output

files from certain applications will automatically be tagged by its DLP system as protected.

Testers noted that jpeg image files could not be protected by the registered document repository classification rule. Files that had fewer than about 350 unique characters also could not be protected. McAfee confirmed that files with these characteristics are not supported.

Trend Micro supports specifying files by various elements of meta data including file types and sizes.

McAfee also supports location-based tagging. In this case, the DLP agent will tag files transferred from particular locations. McAfee also

supports manual tagging. This takes place on the endpoint and it is possible only to tag one file at a time (rather than entire directories).

#### Information Channel Coverage

There are many possible paths across which sensitive data can be leaked to the outside world. A user with malicious intent needs only a single unprotected path available in order to defeat a company’s data loss prevention system. Thus, comprehensive coverage of information channels should be of great importance to security architects.

Threat vectors or “channels” tested included network resources such as email, server shares, web and



instant messenger applications as well as local peripheral devices such as printers, USB and CD/DVD drives.

The Trend Micro DLP solution was able to protect content from exiting the system on all of the aforementioned channels as well as additional channels. Please see Figure 3 for the complete list.

### McAfee Channel Coverage Results

Engineers found the “out of the box” support by McAfee to be more limited than Trend Micro. Some channels were only protected after work with McAfee technical support and the application of software patches to the base system. In other cases, a channel was covered but with limitations. In yet other cases, McAfee claimed a channel was supported but Tolly engineers were unable to make that coverage operational even after technical support involvement and application of McAfee-provided software patches.

While McAfee passed the Outlook email tests, problems began with the web email tests. McAfee does not provide a policy/rule explicitly for protecting webmail. Thus, testers used the “Web Post Protection Rule” as recommended by McAfee.

When the protection was enabled, all outgoing mail, protected and unprotected was intercepted and

Endpoint Data Loss Prevention Information Channel Coverage Tests Defined in Tolly Common Test Plan #1130				
No.	Endpoint Information Channel	Trend Micro DLP V5	McAfee Host DLP V3	Notes for McAfee Solution
1	Email - Outlook inline	✓	✓	
2	Email - Outlook attachment	✓	✓	
3	Email -- Web (http/s) inline	✓	✗	No fix found
4	Email - Web (http/s) attachment	✓	✓	Affects normal browsing
5	Email - SMTP inline	✓	✓	
6	Email - SMTP attachment	✓	✓	
7	Web (http) upload	✓	✓	
8	Web 2.0 upload (AJAX)	✓	✗	
9	Instant Messaging (IM)	✓	✓	
10	File save	✓	✓	No blocking
11	File print	✓	✓	
12	Clipboard copy/paste	✓	✓	
13	Copy to USB drive	✓	✓	
14	Copy to network drive	✓	✓	No blocking
15	Copy from network share of client	✓	✗	
16	Burn to CD/DVD	✓	✓	No Blocking
17	Copy via FTP	✓	✓	tagged files

Legend: ✓ = supported, ✗ = not supported, ✓ = supported with limitations or supported only after application of hotfix.

Note: See methodology overview section to see specific applications tested. Users should test the specific applications used in their environments.

Source: Tolly, January 2010

Figure 3

required user justification before the action was allowed to complete. In fact, even the action of

logging into Gmail triggered a policy violation. While McAfee technical support worked



extensively with Tolly engineers they were unable to provide a fix by the conclusion of testing.

McAfee intercepted SMTP traffic properly when the client platform used was Microsoft platform. When The Bat! 4.x, an alternative email client, was used McAfee did not detect the sensitive data traversing the connection.

While McAfee successfully detected sensitive data attempting to be uploaded to Google Docs, it was unable to detect data being uploaded via Flickr uploader.

McAfee's DLP successfully blocked protected data from being leaked via file print functions as well as via copy functions to USB or via the Windows Clipboard copy/paste function.

While McAfee's solution can monitor for protected data that is being copied or saved to a network drive, it cannot prevent or block that copy/save from taking place.

Additionally, in a situation where a network share is created on the client and another system attempts to copy protected data from the protected endpoint that information is copied without even a notification in the DLP management system. McAfee does not consider such a scenario an appropriate DLP function.

McAfee can only monitor burn activity to CD and DVD burner but does not offer a blocking capability for protected data. Engineers confirmed that this was the case.

Finally, support of FTP was partial and required that engineers configure a "Network Communication Protection" rule to protect FTP port 21. McAfee only claims to protect tagged files across FTP sessions.

Engineers confirmed that tagged files would be detected. Engineers noted that once a protected file was blocked all subsequent FTP connections were blocked.

The McAfee support for removable devices proved problematic. For these devices, McAfee allows the copy to take place and then deletes the copied file if the system determines that it is protected.

The implementation appears not to react quickly enough. Engineers determined that if the USB drive was removed immediately after the copy function was completed, that some protected data could successfully be leaked and, in some cases, without that fact even being logged on the management server. (McAfee offers "normal" and "aggressive" deletion modes. Tests were run in both modes and the results were the same.)

Trend Micro successfully scanned and blocked 70 files of 71 files tested while McAfee missed 7 files. Missed files contained unique data content below that vendor's minimum.

### Detection of Fragmented Data

While the majority of leaks are accidental in nature across standard threat vectors, malicious users pose a serious risk and will look for creative means to leak data. While there are various methods that users can employ in an attempt to obfuscate data, fragmentation is one of the most common.

Users break protected data into smaller pieces in the hope that it becomes invisible to the DLP system. Once all of the pieces are leaked beyond the protected system, the user can reassemble the data. This approach is most likely to be used on unstructured data that is either tagged or fingerprinted. Examples might include legal documents, CAD designs, engineering specs, sales results, pricing info, etc.

In this test, engineers began using a document of unstructured data that was identified as protected using the respective method ("fingerprinting" or "tagging").

Both solutions were able to detect documents even when reduced to 10% of the original content.



McAfee notes that documents need to contain 350 or more unique characters in order to be tracked.

### Regulatory Compliance

Trend Micro provides pre-configured compliance templates like PCI Data Security Standard (PCI-DSS), Gramm-Leach-Bliley Act (GLBA), US Personally Identifiable Information (US PII), SB1386 and Health Insurance Portability and Accountability Act (HIPAA). These templates save administrators' time and reduce false positives.

McAfee provides pre-configured HIPAA and PCI GLBA templates in its system dictionary.

### Ease of Use

Engineers found Trend Micro's DLP management console to be more intuitive using the "Getting Started" workflow as shown in Figure 4. Administrators just have to follow the steps in the workflow to configure and deploy policies.

McAfee does not provide any guidance in the console. Administrators have to spend more time researching McAfee's tagging and classification mechanisms and designing their own workflows.

Trend Micro offers administrators flexibility to combine conditions, channels and actions in any way they want to build policies.

For McAfee, there are more limitations and this will increase administrative overhead and effort. AOL Instant Messenger (AIM) provides a good example. Administrators will need to configure two rules to provide protection. The "Network Communication Protection" rule could block and monitor files larger than 12KB. The "Application File Access" rule could monitor but not block files smaller than this. However, with the effort of configuring two protection rules, only tagged files can be protected. This means that any files that would otherwise be detected using dynamic detection via keywords, regular expressions, etc. would be allowed to leave the system via IM.

Tolly Engineers spent two days to deploy Trend Micro's DLP product and configure all policies for the test.

Tolly Engineers spent five days to finish the initial deployment and protection rules configuration work for McAfee's Host DLP product. Tolly engineers spent another four days working with McAfee's technical support to resolve issues and understand workaround and/or limitations. Overall, the process lasted close to a calendar month.

### Test Methodology Overview

The full test methodology is found in Tolly Common Test Plan #1130. That methodology is updated and expanded on an ongoing basis.

#### DLP Information Channel Coverage

**Email – Outlook:** Configure the outlook to one Microsoft Exchange server. Create one new email with a MasterCard number in the content and send it. Document the reaction of the DLP agent. Create one new email with a protected file attached and send it. Document the reaction of the DLP agent.

**Email – Web (Http/s):** Create one new email with a MasterCard number in the content and send it. Document the reaction of the DLP agent. Create one new email with a protected file attached and send it. Document the reaction of the DLP agent.

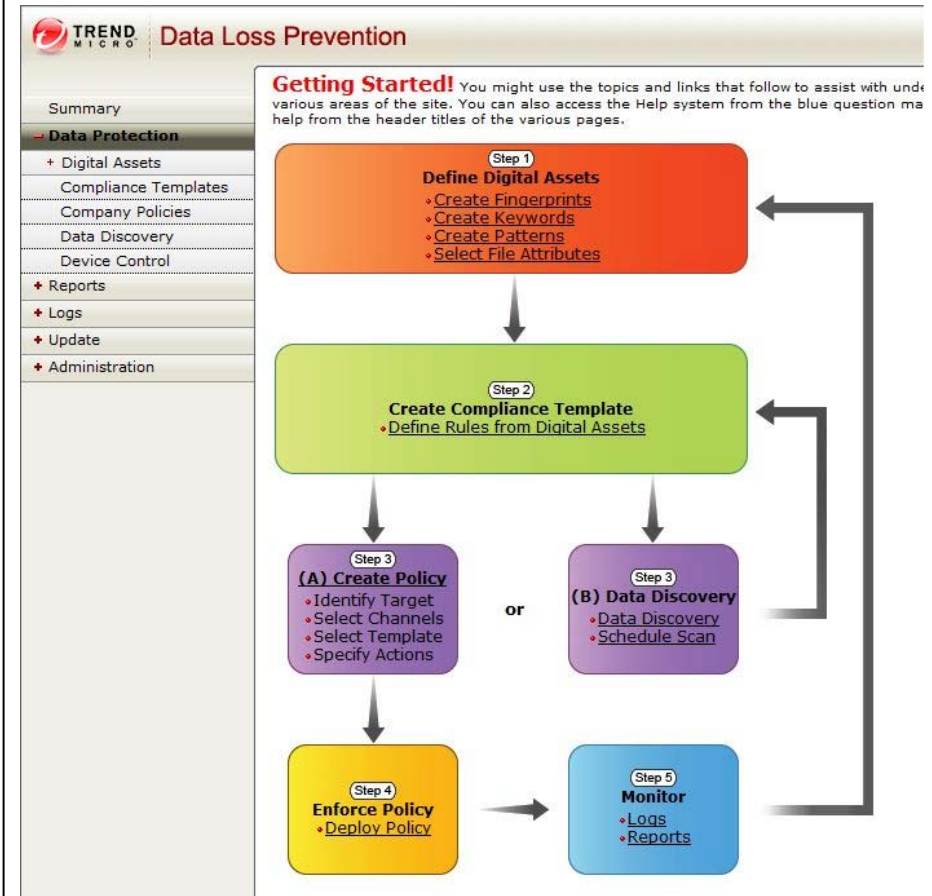


The test methodology used for this report relies upon test procedures, metrics and documentation practices as defined by Tolly Common Test Plan, #1130 Data Loss Prevention

To learn more about Tolly Common Test Plans, go to:

<http://CommonTestPlan.org>

## Trend Micro Data Loss Prevention: Getting Started Workflow



Source: Tolly, January 2010

Figure 4

**Email – SMTP:** Configure the Outlook or other email client to communicate using SMTP with Gmail. Create one new email with a MasterCard number in the content and send it. Document the reaction of the DLP agent. Create one new email with a protected file attached and send it. Document the reaction of the DLP agent.

**File Transfer (FTP):** Transfer one protected file to the FTP server using FileZilla FTP client.

**HTTP Upload:** upload one protected file to Google Docs.

**Web 2.0 Upload (AJAX):** Install Flickr uploader. Upload one protected file to Flickr using the uploader application.

**Instant Messaging:** Transfer one protected file using AIM and Live Messenger.

**File Save:** Save one protected Excel file to flash drive and file server.

**File Print:** Print one protected file.

**Clipboard Copy/Paste:** Copy protected information like a MasterCard number to a newly created text file.

**Copy to USB drive:** Copy a protected file to the USB drive.

**Copy to network drive (CIFS):** Copy a protected file to a network drive on the client's side.

**Copy from network share of client:** Copy a protected file from a file share on the client to the file server on the server's side.

**Burn to CD or DVD:** Tested with CDBurner XP and Nero Express.

## Test Bed Setup

A minimal test environment was required for this evaluation. Generic PCs were loaded with Windows XP SP2 to serve as the protected endpoints.

Dedicated management/policy servers were built for each solution. Please see "Systems Under Test" table for details of the server and software environments.



## About Tolly...

The Tolly Group companies have been delivering world-class IT services for over two decades. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company via E-mail at [sales@tolly.com](mailto:sales@tolly.com), or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at:  
<http://www.tolly.com>

## Competitive Interaction

Tolly engineers shared the test methodologies, configurations used and results with McAfee corporate representatives.



As noted elsewhere in this document, Tolly engineers worked with McAfee technical support to configure the DLP in the manner they recommended as well as applied hotfixes and software patches as directed by McAfee.

For more information on the Tolly Fair Testing Charter, visit:  
<http://www.tolly.com/FTC.aspx>

## Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.