#210147
September 2010
Commissioned by Symantec Corporation

The Total Cost of Ownership of Data Loss Prevention:

Symantec DLP v10.5 vs. McAfee Host and Network DLP v9.0

Executive Summary

Symantec commissioned Tolly to perform a head-to-head evaluation of Symantec Data Loss Prevention 10.5 vs. McAfee Data Loss Prevention 9.0. Both solutions were installed by technicians certified by the respective company. McAfee was invited to participate in the testing, but declined. (See Fair Testing Charter section below for more information.)

The goal of this comparison was to examine key elements of both solutions and understand the impact on the Total Cost of Ownership (TCO) of the solutions.

The test focused on key areas that can impact TCO:

1) incident remediation workflow

2) detection accuracy

3) network monitoring performance

4) solution deployment.

Overall in the tests described in this document, Symantec Data Loss Prevention demonstrated:

25% less time to resolve data loss incidents with an integrated management console

32% higher accuracy when detecting US Social Security Numbers

53% higher network monitoring performance with no false positives

The Bottom Line

Symantec Data Loss Prevention v10.5:

1 Provided more rapid remediation than McAfee DLP

2 Provided fully integrated host and network data loss prevention solution with one management console

3 Detected 100% of sensitive data while processing ~640Mbps of background traffic compared with McAfee's limit of ~300Mbps of background traffic

4 Identified protected data in a test dataset of US Social Security Numbers more accurately than McAfee DLP

5 Demonstrated more flexible deployment as software/virtual appliances vs McAfee's physical appliances

Introduction

The focus of this project was to build a microcosm of an enterprise data loss prevention solution with current offerings from Symantec Corporation and McAfee, Inc. and compare key elements of the competing solutions. The DLP solutions included both host (endpoint) and network data loss prevention elements. Systems were built to each company's specifications.

Summary of Findings

Incident Remediation Workflow

Once an incident is correctly identified, it is important to understand what tools each vendor provides to help remediate the situation.

For 100 endpoint incidents, 100 network incidents and 100 storage incidents, Tolly engineers took approximately 3 hours to remediate on the Symantec solution and 4 hours on the McAfee solution.

Both systems support policy violation detection, incident status, protocol, severity, sender (offender), recipient, application, etc.

Symantec supports a built-in LDAP and CSV lookup in the incident snapshot. Administrators can identify attributes of the offender and make the first response very quickly using smart response actions like notifying the manager and the sender (offender) with several clicks. McAfee NDLP v9.0 can leverage McAfee Logon Collector to resolve user identities from Active Directory servers. McAfee, however, does not provide a smart response feature on the incident page. Thus, administrators have to manually write the email to notify manager and offender. With a large number of incidents this can add considerably to the time required for remediation.

According to McAfee help files, reviewer is the only option available on McAfee Network DLP Discover for automatic email notification. Also, as McAfee Host Data Loss Prevention (HDLP) and Network Data Loss Prevention (NDLP) are still not fully integrated, administrators will not be able to identify user attributes for data in use if HDLP and NDLP are used separately in McAfee ePolicy Orchestrator (ePO) 4.5. Symantec automatic response does not have similar restrictions.

For the remediation process, a Tolly engineer first identified attributes of the incident, then notified the offender and manager, and finally modified the status of the incident and made comments. For both systems, user attributes lookup and automatic response require significant configuration work and may not work for all incidents. So, Tolly engineers preferred to use manual first response for each incident.

Symantec Corporation

Symantec DLP v10.5

Data Loss Prevention Solution Comparison

Tolly. Certified

Tested August 2010

McAfee HDLP and NDLP can both be managed from McAfee ePO but are two applications that are not fully integrated. Users of what McAfee terms Unified DLP (integrated HDLP and NDLP) will lose several HDLP features.

Symantec and McAfee Data Loss Prevention Solution Components

	Components	Version	Notes
Symantec	Enforce Platform, Network Discover, Network Monitor, Network Prevent for Email and Web, Endpoint Prevent	10.5 for all components	Network Monitor must be one dedicated server, Enforce is one dedicated server, Endpoint is one dedicated server,Network Prevent for Email, Network Prevent for Web, Network Discover are implemented as virtual appliances in this test environment.
McAfee	Network DLP Manager, Network DLP Discover, Network DLP Monitor, Network DLP Prevent, ePO 4.5 (with Host DLP extension)	9.0 for all DLP components, 4.5 for management system	Components were implemented in the following appliances: Manager 1650, Discover 3650, Monitor 3650, Prevent 3650. ePolicy Orchestrator ran on a standard Dell Inspiron 530S machine

Source: Tolly, August 2010

Table 1

The only remediation actions available for incidents in the HDLP monitor are setting the label and sending an email report. Administrators have to look for the users' information manually. The McAfee NDLP Report page can integrate an LDAP server to look for users' attributes.

Detection Accuracy

Symantec DLP Network Monitor and Endpoint Prevent detected confidential data accurately 100% of the time. They correctly generated incidents for all the valid US Social Security Numbers (SSNs) and did not generate any incidents for the invalid SSNs.

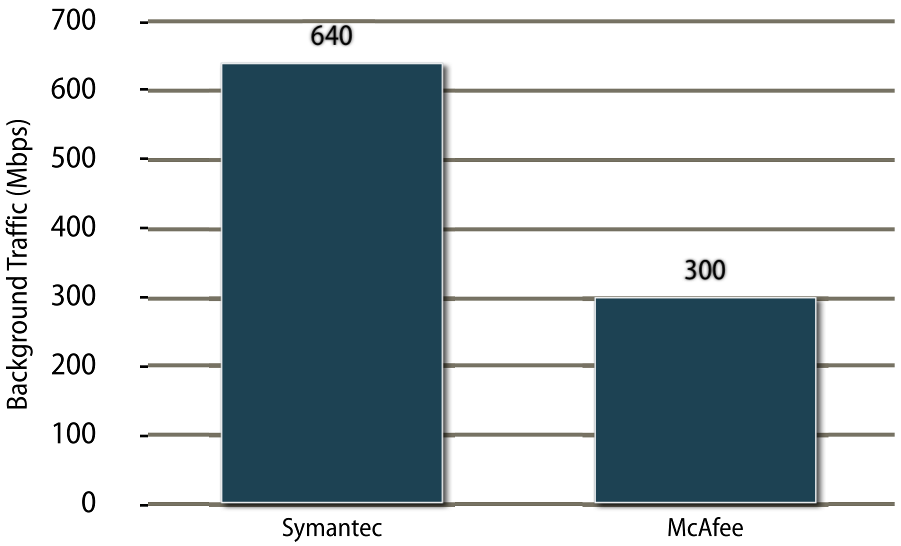
McAfee Host and Network DLP only detected confidential data accurately 69% of the time. They correctly generated incidents for all the valid SSNs, however, they falsely generated incidents for the 31 files containing invalid SSNs.

During the evaluation, McAfee and Symantec each inspected 100 files containing SSNs; of those, 31 files contained invalid SSNs to test for false positives.

Higher accuracy can translate into lower TCO. DLP detection accuracy matters because if your DLP system makes mistakes you're wasting resources chasing down false alarms (or false positives). False positives cause security personnel to waste time; they also adversely impact user productivity by potentially blocking non-sensitive emails and uploads. False negatives allow confidential data to leave the company.

Detection accuracy is measured in terms of false negatives and false positives (along with true positives and true negatives) – like medical test results. A false positive means the email contained confidential data, when in reality it didn't. A false negative means the email did not contain confidential data, when in reality it did.

Symantec vs. McAfee Network DLP
100% Incident Detection vs Background Traffic Levels
Gigabit Ethernet Monitor Port Traffic in One Direction



Note: Engineers used the Tcpreplay utility to send background traffic repeatedly at levels up to those noted in the graph. After the background traffic began engineers used the same utility to send a file at a rate of ~17 to 19Mbps containing a single email (SMTP) with 7,354 instances of the string "confidential123" occurring in the email. At 300Mbps of background traffic, McAfee began reporting zero incidents in some test runs. Above the 450Mbps level, McAfee had a zero detection rate in all test runs and the monitor was functionally bypassed.

Source: Tolly, August 2010

Figure 1

Network Monitoring Performance

Network DLP monitors traffic flowing across the LAN to identify potential data loss. The network monitor component is typically placed on the backbone of the network to maximize the traffic coverage for the system. Such backbone links will, at a minimum, be Gigabit Ethernet and potentially carry traffic loads in the hundreds of megabits per second either on a regular basis or in bursts.

The traffic load is important because the network monitor must use deep packet inspection, a resource-intensive task, to scan packet content in search of sensitive material. It is important for security architects to understand how much traffic can be processed before the devices start failing at detecting valid security incidents.

The Symantec solution was able to detect 100% of the 7,354 instances of sensitive data while processing background traffic of 640 Mbps. This result was in marked contrast to the McAfee solution that peaked at 300 Mbps. In fact, at that rate the McAfee solution detected 100% of the matches in only five out of 10 test runs. In the other 5 test runs, no incidents were detected. See Figure 1.

While the design goal should always be to detect 100% of incidents and matches, it is instructive to see how solutions operate once their processing levels are exceeded.

Tolly engineers tested up to a background load of 724Mbps - the point where the traffic generator maxed out. Even at this traffic rate, the Symantec solution detection 7,144 matches or 97.14% accuracy.

Symantec vs McAfee
US Social Security Number Detection Accuracy
100 Total Files Containing Valid and Invalid SSN numbers

		BLocked	Passed			
		Valid SSN	Invalid SSN Non-issued Range	Invalid SSN Area Number Mismatch	Blank Files	Accuracy (%)
Correct Results		62	31	5	2	N/A
Symantec	Host DLP	62	31	5	2	100
	Network DLP	62	31	5	2	100
McAfee	Host DLP	62 valid , 31 non-issued range and 1 area number mismatch blocked (32 false positives)	0	4	2	68
	Network DLP	62 valid and 31 non-issued range blocked (31 false positives)	0	5	2	69

Note: SSN ranges can be validated using data publicly available on the US Social Security Administration website at http://www.ssa.gov/employer/ssns/HGJan0410.txt.

Source: Tolly, August 2010

Table 2

The McAfee results were very different. When engineers generated background traffic above the 300Mbps referenced earlier, the McAfee solution reported zero incidents in some test runs. When background traffic was increased to 450Mbps, the McAfee solution reported zero incidents in all test runs. Thus, it appears that at this level, the system is functionally bypassed as no incidents at all are detected.

Higher throughput will likely translate to lower TCO as fewer network DLP devices will need to be deployed to provide equivalent data coverage. This is of particular importance to organizations that anticipate high levels of traffic on the network.

Solution Deployment

Significantly, the Symantec approach allows customers to leverage virtualization technology by running components as virtual appliances along with unrelated appliances in a virtualized server environment.

Both solutions require similar components to monitor traffic, discover sensitive data, prevent sensitive data from leaking and manage the DLP services on both hosts (endpoints) and DLP servers. See Table 1 for a list of components evaluated.

As noted above, the primary difference between the solutions is that McAfee delivers all of its DLP components except its management system bundled as hardware appliances where Symantec is a software-only solution. While some Symantec components require dedicated servers, it does allow the customer to match the server with the DLP requirement and upgrade hardware independent of the DLP vendor.

Test Bed Setup

Symantec and McAfee DLP solutions were built into two domains. Each test bed has one domain controller, one DNS server, one Exchange server, one Web proxy and one email proxy. All components were configured to work with DLP products appropriately by vendor trained technician. Please see figure 2 for detailed information.

Test Methodology

Network Performance

One HP ProLiant DL360 G5 server with two dual-core Intel® Xeon® 5140 2.66-GHz, 14 GB RAM, 72 GB HDD and Ubuntu Linux Release 9.10 was used as the traffic generator. Tcpreplay version 3.4.1 (build 2229) tool was used to send background and incident traffic. The traffic generator was directly connected to the monitor port of the Network DLP Monitor appliance under test.

Tolly engineers tested the detection limits of both vendors' network DLP solutions by transmitting sensitive traffic at rate of less than 20Mbps into the monitor port of each device while simultaneously transmitting background traffic starting at low rates. The tests were run repeatedly with the background traffic increasing until the network DLP solution failed to identify 100% of the incidents. After that point, engineers increased the background traffic to determine a second data point where approximately 95% or more of the incidents could be detected by the solution.

One 826 MB file Large.pcap with pre-captured network traffic in an enterprise environment was used as the background traffic. One 21.4 MB file trap2incidents.pcap with one SMTP email message traffic was used as the incident file. The email message contains 7354 instance of the string "confidential123" that violated policies on both Symantec and McAfee Network DLP Monitors.

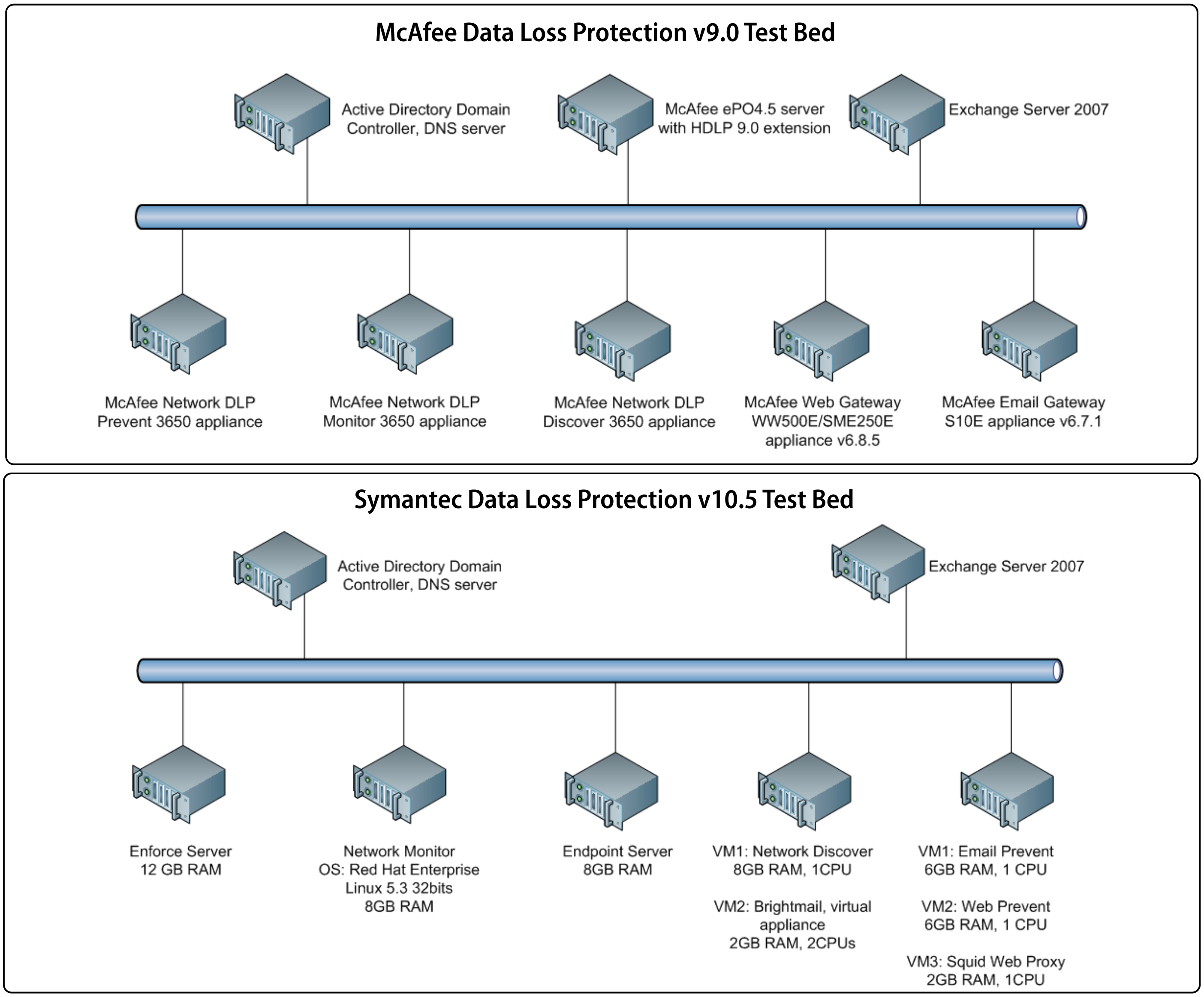
Tolly Engineers sent out the Large.pcap background traffic file looped three times. The incident traffic file trap2incidents.pcap file was sent out during the second loop of the Large.pcap file.

Detection Accuracy

"Data in use" accuracy was tested by sending test files to one flash drive. "Data in motion" accuracy was tested by uploading test files to Google Docs via HTTP.

Default data identifier US Social Security Number (SSN) with wide breadth was used for Symantec. Default concept SOCIAL-SECURITY-NUMBER-GENERAL was used for McAfee NDLP. Default text pattern Social Security Number was used for McAfee HDLP.

Data Lost Prevention Test Bed Overview


McAfee Data Loss Protection v9.0 Test Bed
Active Directory Domain Controller, DNS server
McAfee ePO4.5 server with HDLP 9.0 extension
Exchange Server 2007
McAfee Network DLP Prevent 3650 appliance
McAfee Network DLP Monitor 3650 appliance
McAfee Network DLP Discover 3650 appliance
McAfee Web Gateway WW500E/SME250E appliance v6.8.5
McAfee Email Gateway S10E appliance v6.7.1
Symantec Data Loss Protection v10.5 Test Bed
Active Directory Domain Controller, DNS server
Exchange Server 2007
Enforce Server 12 GB RAM
Network Monitor OS: Red Hat Enterprise Linux 5.3 32bits 8GB RAM
Endpoint Server 8GB RAM
VM1: Network Discover 8GB RAM, 1CPU
VM2: Brightmail, virtual appliance 2GB RAM, 2CPUs
VM1: Email Prevent 6GB RAM, 1 CPU
VM2: Web Prevent 6GB RAM, 1 CPU
VM3: Squid Web Proxy 2GB RAM, 1CPU

Notes: 1. All McAfee components are appliances. All servers used for Symantec solution are HP DL360G5 servers outfitted with two dual-core Intel® Xeon® 5140 2.33-GHz processors and 72GB HDD.

2. All Symantec DLP products excluding Network Monitor were installed on Microsoft Windows Server 2003 R2 SP2 32-bit Enterprise Edition.

3. Virtual Machines were running on VMware ESX Server 3.5.0.

Source: Tolly, August 2010

Figure 2

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by e-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

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

Interaction with McAfee, Inc.

In accordance with our process for conducting comparative tests, The Tolly Group contacted McAfee, Inc. to notify them of the evaluation and invite their participation. A management representative of McAfee, Inc. respectfully declined to participate in the test.

As noted elsewhere in this document, a trained CDW technician installed the solution and McAfee Gold Technical Support assisted in resolving technical issues.

Tolly. Fair Testing Charter

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.