National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5

Report Number: CCEVS-VR-VID10377-2011
Dated: 14 October 2011
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome F. Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 was performed by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in August 2011.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by McAfee, Inc. The ETR and test report used in developing this validation report were written by COACT. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, dated September 2007 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R2, dated September 2007. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is a host-based intrusion prevention system designed to protect system resources and applications, and includes a host based management system that provides management and monitoring functionality. HIP works to intercept system calls prior to their execution and network traffic prior to their processing. If the HIP Agent determines that a call or packet is symptomatic of malicious code, the call or packet can be blocked and/or an audit log record created. If the TOE determines that a call or packet is safe, it is allowed.

The McAfee Agent and HIP software are installed on the host to be protected. The HIP software is operating system specific. Only the Windows version is included in this evaluation. ePO distributes and manages agents that reside on client systems. A centralized but distributed architecture allows the HIP software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality. Based upon per-user permissions, users may configure the policies to be enforced on individual systems (executing the HIP software).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5
Protection Profile	Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSPP).
Security Target	*Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Security Target*, version 1.0, August 18, 2011
Dates of evaluation	September 2009 through August 2011
Evaluation Technical Report	*Evaluation Technical Report for the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5*, Document No. E2-0411-022, 10 August 2011
Conformance Result	Part 2 conformant and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R2, September 2007 and all applicable NIAP and International Interpretations effective on December 17, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on December 17, 2008
Sponsor	McAfee, Inc., 2821 Mission College Blvd., Santa Clara, California 95054
Developer	McAfee, Inc., 2821 Mission College Blvd., Santa Clara, California 95054
Common Criteria Testing Lab	COACT Inc. CAFÉ Labs, Columbia, MD
Evaluators	Greg Beaver, Brian Pleffner, Dave Cornwell and Jonathan Alexander
Validation Team	Dr. Jerome Myers and Mike Allen of The Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 Security Policy

The security requirements enforced by the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 were designed based on the following overarching security policies:

3.1 Audit

The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user. The TOE audit functionality includes the ability to configure what auditable events generate audit records.

3.2 Identification and Authentication

The TOE requires administrative users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

3.3 Management

The TOE's Management Security Function provides administrator functionality that enables a human user to configure and manage TOE components. Configuration functionality includes enabling a user to modify TSF Data. Management functionality includes invocation of TOE functions that effect security functions and security function behavior.

3.4 System Protection

The Agents are host based intrusion prevention systems designed to protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and comparing them to signatures symptomatic of known attacks and behavioral rules. The Agents also inspect network traffic by comparing packets to signatures symptomatic of known attacks. If a potential security violation is detected, the system call or network traffic may be allowed to proceed or be blocked. An audit event may also be generated.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraphs were made during the evaluation of McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5.

4.1 Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- The TOE includes McAfee Host Intrusion Prevention for Desktops as well as McAfee Host Intrusion Prevention for Servers. Both are the same software/code base; the latter provides SQL and IIS protection when a server operating system is detected during install.
- Only the windows version is covered by this evaluation.
- The functionality not included in the evaluation is itemized below:
    - Firewall functionality (some government users require firewall functionality to be disabled unless it has been evaluated against one of the firewall PPs at EAL4 or Medium Robustness). Application blocking functionality is associated with the firewall functionality and is also excluded.
    - Custom signatures and policies.
    - Importing configurations.
    - HIP Solaris Agents.
    - HIP Linux Agents.

5 Architectural Information

The TOE's evaluated configuration consists of a single instance of the management system (with ePO) and one or more instances of managed systems (with McAfee Agent and the HIP Agent). The following list itemizes configuration options for the TOE for the evaluated configuration:

1. ePO supports both ePO authentication and Windows authentication of user account credentials. The evaluated configuration requires the use of ePO authentication only.
2. The ePO application executing on a dedicated server
3. The McAfee Agent and HIP software on each system to be protected.

The following table identifies the minimum hardware and software requirements for components provided by the IT Environment:

Table 1 - Hardware and Software Requirements for IT Environment

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	HIP Agent 8.0 (for Servers and for Desktops) ePolicy Orchestrator 4.5 Patch 3 McAfee Agent 4.5[1] Patch 2 Database Capacity Monitor Extension 1.0

Table 2 - McAfee Agent and HIP Hardware/Software Requirements

Minimum Requirements	
Windows XP Professional with SP2, SP3	X86 platforms
Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (all editions)	X86 and X64 platforms
Windows Vista SP1 (Business, Enterprise, Ultimate editions)	X86 and X64 platforms
Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2	X86 and X64 platforms
Windows 7 (Professional, Enterprise, Ultimate editions)	X86 and X64 platforms

[1] McAfee Agent 4.5 is shipped/packaged with ePO 4.5. From a clean installation, no additional steps are necessary to install McAfee Agent 4.5.

Table 3 - ePO Hardware/Software Requirements

Minimum Requirements	
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM
Free Disk Space	1 GB
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Web with Service Pack 2 or later Windows Server 2003 R2 Enterprise with Service Pack 2 or later Windows Server 2003 R2 Standard with Service Pack 2 or later Windows Server 2008 Enterprise Windows Server 2008 Standard

6 Documentation

This section provides a listing of the IT product documentation provided with the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 by the developer to the consumer or available from McAfee on their web site. Each was downloaded, evaluated and considered part of the vendor delivered evidence.

1. McAfee ePolicy Orchestrator 4.5 Installation Guide, 2009
2. McAfee Host Intrusion Prevention 8.0 Installation Guide, 2010
3. McAfee ePolicy Orchestrator 4.5 Product Guide, 2009
4. McAfee Host Intrusion Prevention 8.0 Product Guide for use with ePolicy Orchestrator 4.5, 2010
5. Operational User Guidance and Preparative Procedures Supplement McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5, Document Version 2.0, August 18, 2011

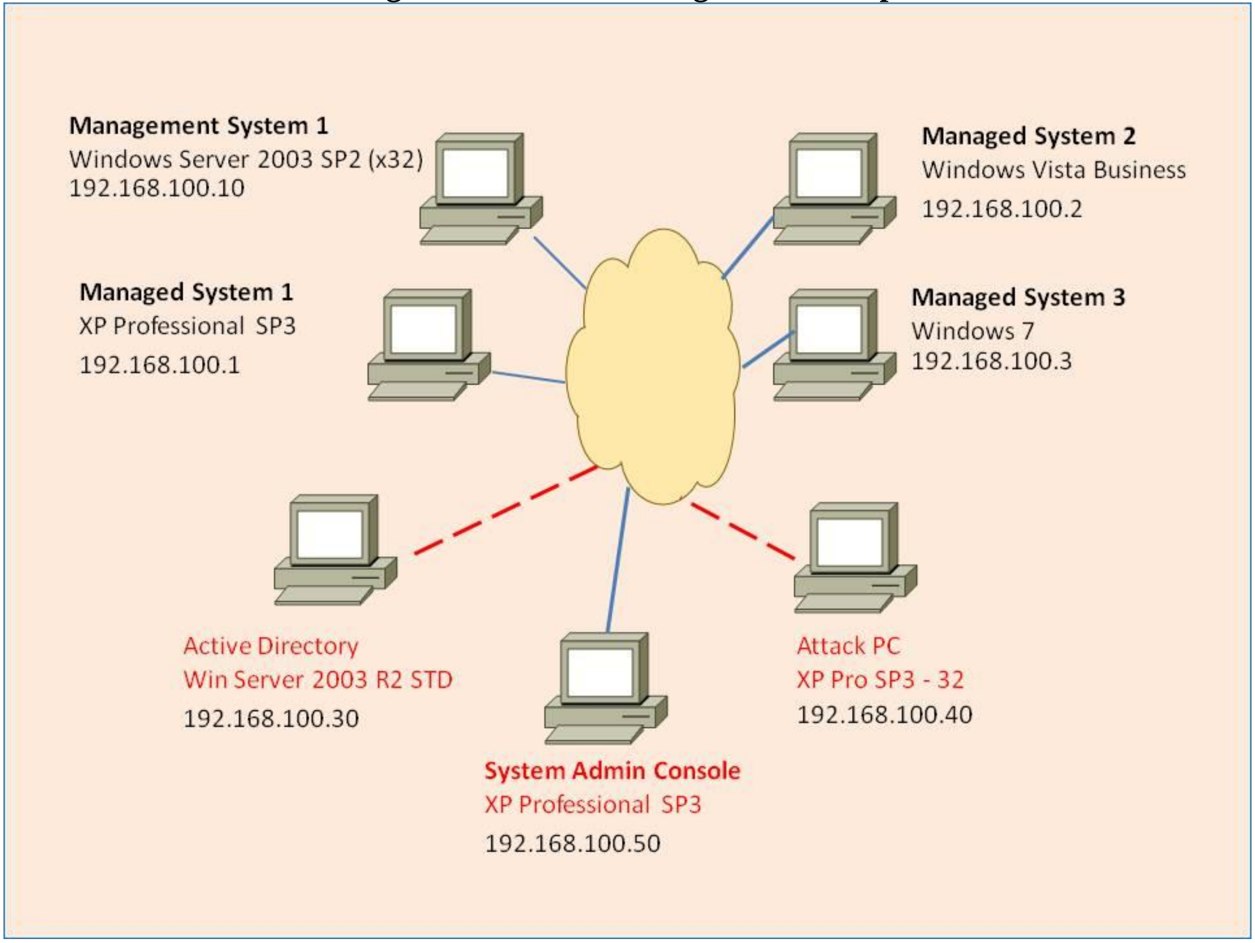
7 IT Product Testing

Testing was completed on August 1, 2011 at the COACT CCTL in Columbia, Maryland. COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

Figure 1 - Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 4 - Test Configuration Overview

System	Purpose
Management System 1	System on which the ePO management system is installed.
Managed System 1	The managed host with XP installed.
Managed System 2	The managed host with Vista installed.

System	Purpose
Managed System 3	The managed host with Windows 7 installed.
Active Directory	Computer to provide the Active Directory and DNS Server services.
Attack PC	Computer from which the penetration tests will be launched against the TOE.
System Admin Console	Computer from which the ePO is managed through the Web browser.

Specific configuration details for each of the systems are provided in the tables below.

Table 5 - Management System 1 Details

Management System Requirements	
Installed Software	Windows 2003 Server with SP2 ePolicy Orchestrator 4.5, Patch 3 (provides management and authentication) McAfee Agent 4.5, Patch 2 MS SQL Server Service Manager 8.00 HIP Client 8.0 SnagIt 8 Libre Office 3.3

Table 6 - Managed System 1 Details

Managed System 1 Requirements	
Installed Software	Windows XP Professional with SP3 McAfee Agent 4.5, Patch 2 HIP client 8.0 SnagIt 8 Libre Office 3.3

Table 7 - Managed System 2 Details

Managed System 2 Requirements	
Installed Software	Windows Vista SP1 McAfee Agent 4.5, Patch 2 HIP client 8.0 SnagIt 8 Libre Office 3.3

Table 8 - Managed System 3 Details

Managed System 3 Requirements	
Installed Software	Windows 7 McAfee Agent 4.5, Patch 2 HIP client 8.0 SnagIt 8 Libre Office 3.3

Table 9 - Attack PC Details

Item	Purpose
Installed Software	Windows XP Professional SP3 Internet Explorer 6.0 SP1or later WinZip 10 ZENMAP GUI 5.21 Nmap 5.21 NEWT 3 SnagIt 8 WireShark 1.4.0 Nessus Version 4.2 SnagIt 8 Libre Office 3.3

Table 10 - Active Directory & DNS Server Details

Item	Purpose
Installed Software	Microsoft Windows 2003 Server R2 STD Mail Enable Standard Edition Version 1.986.0.0 SnagIt 8 Libre Office 3.3

Table 11 - System Admin Console Details

Item	Purpose
Installed Software	Windows XP Professional with SP3 Internet Explorer 6.0 SP1or later SnagIt 8 Libre Office 3.3

7.2 Functional Test Results

The team repeated the developer test suite including all of the developer functional tests. Additionally, each of the Security Functions and developer tested TSFI were included in the CCTL test suite. The results are found in McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Test Report, dated August 1, 2011.

7.3 Evaluator Independent Testing

The tests chosen for independent testing allowed the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests was to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allowed for a finer level of granularity of testing compared to the developer's testing, or provided additional testing of functions that were not exhaustively tested by the developer. The tests allowed specific functions and functionality to be tested. The tests reflected knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests.

7.4 Evaluator Penetration Tests

The evaluator consulted vulnerability relevant sources of information to verify that the developer did not have any obvious vulnerabilities identified for the TOE. These sources included:

A) http://osvdb.org/

B) http://www.securityfocus.com/

C) http://secunia.com/

D) http://web.nvd.nist.gov

Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

7.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 running the client on a PC running one of Microsoft Windows XP Professional with Service Pack 3, Windows Vista (32-bit or 64-bit) with service pack 1, or Windows 7 (32-bit or 64-bit) operating systems and the manager on a PC running one of the 64-bit variants of Microsoft Windows Server 2008 with Service Pack 1 and any variant of Microsoft Windows Server 2003 with Service Pack 2.

9 Results of the Evaluation

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the product for selected developer identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Test Report, dated August 1, 2011.

The evaluation determined that the product meets the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The TOE includes McAfee Host Intrusion Prevention for Desktops as well as McAfee Host Intrusion Prevention for Servers. Both are the same software/code base; the latter provides SQL and IIS protection when a server operating system is detected during install.
- Only the windows version is covered by this evaluation.
- The functionality not included in the evaluation is itemized below:
    - Firewall functionality (some government users require firewall functionality to be disabled unless it has been evaluated against one of the firewall PPs at EAL4 or Medium Robustness).
    - Application blocking functionality is associated with the firewall functionality and is also excluded.
    - Custom signatures and policies.
    - Importing configurations.
    - HIP Solaris Agents.
    - HIP Agents.

11 Security Target

The Security Target is identified as the McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Security Target, Version 1.0, August 18, 2011. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organizations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R2, September 2007.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- McAfee Host Intrusion Prevention (HIP) 8.0 and ePO 4.5 Test Report, July 12, 2011, Document No. E2-0411-021.
- Evaluation Technical Report for McAfee HIP 8.0 and ePolicy Orchestrator 4.5, August 10, 2011, Document No. E2-0411-022.
- McAfee Host Intrusion Prevention 8 and ePolicy Orchestrator 4.5 Security Target, Version 1.0, August 18, 2011.