



Maintenance Report

McAfee Network Data Loss Prevention 9.3

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2013

Document number:	383-7-99-MR
Version:	1.0
Date:	25 October 2013
Pagination:	1 to 2

1 Introduction

McAfee, Inc. has submitted (via Apex Assurance Group) the Impact Analysis Report (IAR) for McAfee Network Data Loss Prevention 9.3 (hereafter referred to as McAfee NDLP), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in McAfee NDLP, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes in the Maintained Target of Evaluation

The following characterizes the changes implemented in McAfee NDLP. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in McAfee NDLP comprise bug fixes resulting from defects detected and resolved through the QA/test process as well as new features and enhancements to existing functionality. None of the changes affect the security claims in the Security Target.

3 Description of Changes to the IT Environment

Changes to the product outside the TOE boundary are permissible under assurance continuity provided that they do not change the certified TOE. In this case one new model was added to the instances of the TOE that operate in the Common Criteria (CC) configuration. This model is the 5500 Appliance. None of the changes affect the security claims in the Security Target.

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

5 Conclusions

All changes to the maintained TOE were bug fixes and performance improvements. Through functional and regression testing of McAfee NDLP, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

6 References

Assurance Continuity: CCRA Requirements, v2.1, June 2012.

CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011.

Certification Report EAL 2+ Evaluation of McAfee Network Data Loss Prevention v1.0, 14 March 2012.