Maintenance Report

McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

1   Introduction

McAfee Inc., via EWA-Canada, has submitted the Impact Analysis Report (IAR) for McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.3 (hereafter referred to as McAfee Enterprise Security Manager), 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 Enterprise Security Manager, (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 to the Maintained Target of Evaluation

The following characterizes the changes implemented in McAfee Enterprise Security Manager. 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 Enterprise Security Manager comprise;

- bug fixes and feature enhancements resulting from defects detected and resolved through the QA/test process;

3   Description of Changes to the IT Environment

Changes to the IT Environment are permissible under assurance continuity provided that they do not change the certified TOE. A modified ST was provided which listed the updated software. McAfee Inc. subjected the TOE to complete regression testing. The changes to the IT Environment included:

- Support for new database servers;

- Additional User Interface language support;

- Availability of the Application Data Monitor (ADM) and Database Event Monitor (DEM) on virtual machines; and

- Support for collecting logs from Windows 8 and Windows Server 2012.

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

Through functional and regression testing of McAfee Enterprise Security Manager, 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;
- Certificate of Product Evaluation McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1, version 1.0, 27 November 2013;
- Security Target McAfee Enterprise Security Manager with Event Receiver, Enterprise Log Manager, Advanced Correlation Engine, Application Data Monitor and Database Event Monitor 9.1 version 1.1, 25 March 2013