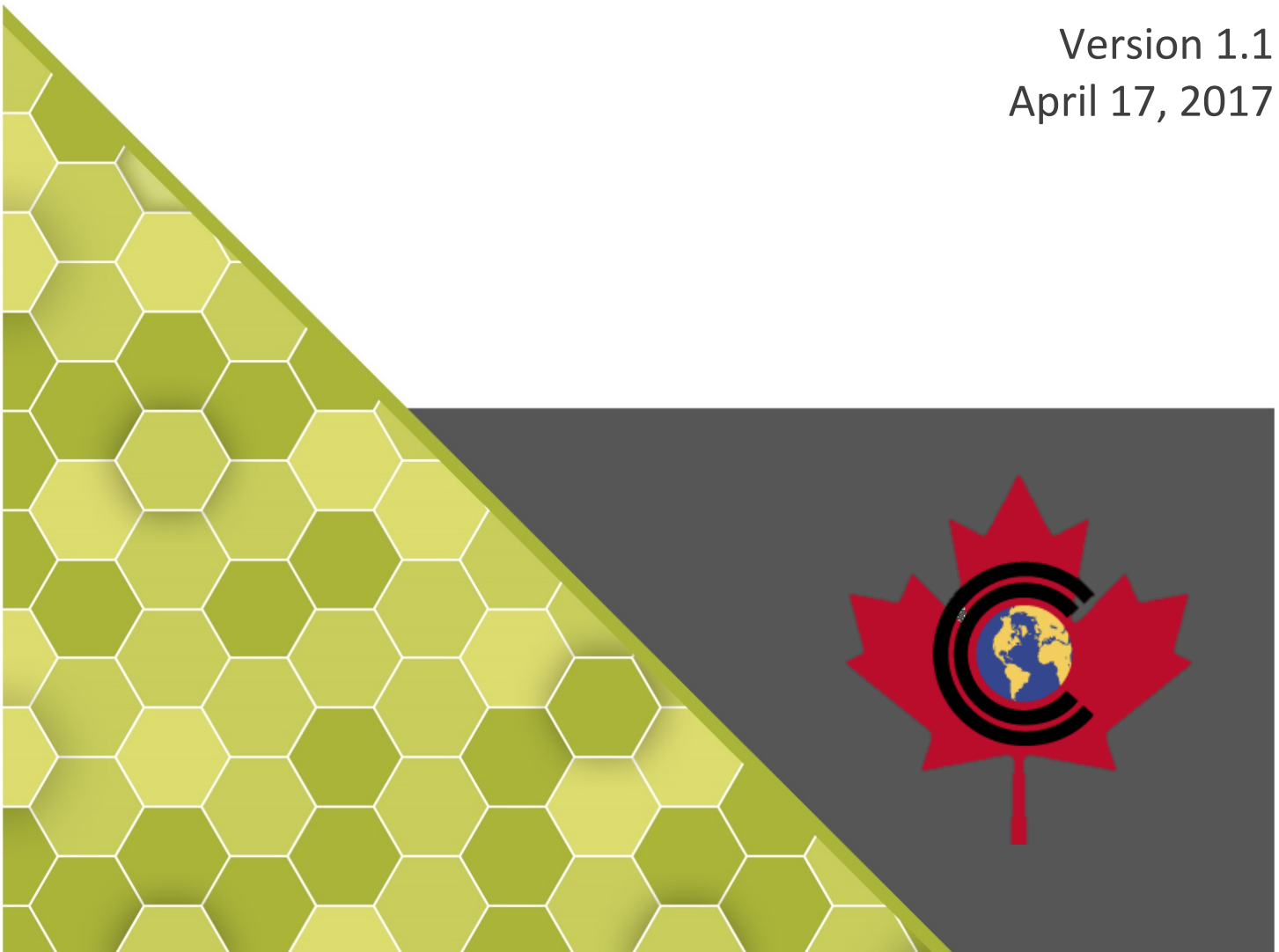




# COMMON CRITERIA MAINTENANCE REPORT

McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2

Version 1.1  
April 17, 2017





# FOREWORD

The *Document Name* is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

If your department has identified a requirement for report based on business needs and would like more detailed information, please contact:

ITS Client Services

Telephone: (613) 991-7654

E-mail: [itsclientservices@cse-cst.gc.ca](mailto:itsclientservices@cse-cst.gc.ca)



## OVERVIEW

McAfee, Inc. has submitted the Impact Analysis Report (IAR) for McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 (hereafter referred to the TOE), 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 the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.



# TABLE OF CONTENTS

<b>1</b>	<b>Changes</b> .....	<b>5</b>
1.1	Description of changes in the Maintained Target of Evaluation .....	5
1.2	Affected developer evidence.....	5
<b>2</b>	<b>Conclusions</b> .....	<b>6</b>
2.1	References .....	6



# 1 CHANGES

The following characterizes the changes implemented in the TOE and/or the environment. 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.

## 1.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise;

- Updated McAfee Endpoint Security software to 10.5.0
- Updated ePolicy Orchestrator software to 5.3.2 with the following hotfixes applied:
  - #1159423
  - #1151890
  - #1144868
- Updated McAfee Agent software to 5.0.4 with the following hotfix applied:
  - #1174804
- Updated Apache server to 2.4.16;
- Restriction on the use of TLS 1.0;
- Fixes for Denial-of-service and cross-site scripting attacks;
- OpenSSL updated to 1.0.2j (ePO);
- RSA BSAFE Micro Edition Suite updated to 4.0.1;
- Additional features not included within the scope of the evaluation; and
- Enhanced IPS functionality

## 1.2 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.



## 2 CONCLUSIONS

Through functional and regression testing of the TOE, 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.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

### 2.1 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report: McAfee Endpoint Security 10.1.0 with ePolicy Orchestrator 5.3.1, v1.0, 3 June 2016
McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 security target v1.8, 17 April 2017