



CHECKMARK CERTIFIED

## TEST SUMMARY

Technology: Anti-malware  
Advanced System Repair  
Date: 24<sup>th</sup> October 2018  
Document Version: 1.0



## Introduction

This document is designed to provide a high-level outline of the testing requirements and procedures that form the Checkmark Certified Verified Genuine Solution accreditation.

This accreditation should not be taken in isolation as an indication of a solution's protection capability; but is, instead, designed to show that the solution under test is a genuine application and not malicious.

It is recommended that this accreditation be combined with that of Checkmark Certified Anti-Malware Desktop.

All information contained within this document shall remain the property of Checkmark Certified.

## About Checkmark

The Checkmark Certified (CC) business philosophy is founded on quality and excellence with all testing activities carried out in a secure, real-world test environment and within a framework of confidentiality that ensures integrity of information and test data.

CC prides itself on its open and proactive working relationship with all its clients through ongoing and meaningful communication.

The outcome is a sound technical working relationship, which ensures the client derives maximum benefit from engaging with an independent test facility that can also act as a conduit to a global buying market for security products and services



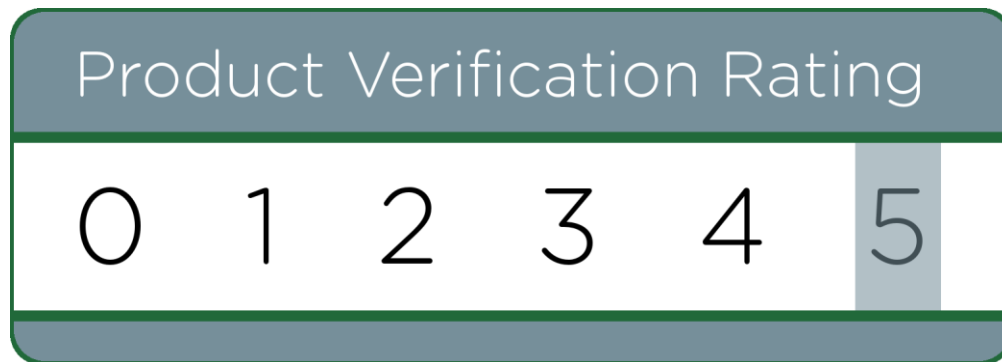
## Test Overview

Each solution that attains Verified status under the Checkmark Certified scheme, must meet a set of criteria designed to show that the solution in question is a genuine security solution and takes steps to attempt to better the current level of security.

Unlike our certification and custom test reports, the Verified scheme and its various criteria are not designed to provide a performance benchmark.

Outlined below are those areas that are examined as part of the Verified testing and any failure points that may be encountered.

## Test Result



## Test Criteria

### Security Protection

As a bare minimum, the solution must be able to demonstrate that it is able to detect any attacks for which it is designed. There is no pass/fail threshold for this unless this solution is subsequently entered into Checkmark Certified's certification scheme. Furthermore, the solution must be able to demonstrate that updates to its security protection are made available on a regular basis.

Attacks Detected: VERIFIED

Regular Updates: VERIFIED

## System Overhead


While primary concern must obviously lie in the solution's ability to provide the security protection for which it is advertised, this must not come at the cost of the host system's usability or performance. Doing so may result in the user(s) subsequently disabling certain parts of the solution and compromising its capability.

To determine the solution's impact, the following areas are examined under a number of different scenarios; each of which is designed to mimic common interactions carried out by either a home or corporate user. The interactions include web browsing, file extraction, system reboots, office and application use.

System Reboots:  VERIFIED

CPU Use:  VERIFIED


Memory Use:  VERIFIED


Network Impact:  VERIFIED

## Personal Information

At the heart of the Verified scheme, is the determination of whether the solution's behaviour, whether by design or by accident, makes the user vulnerable to information and/or identity theft.

This may be carried out in one of several ways, with the Verified scheme specifically looking at the capture of financial data, such as credit card numbers, or personal information that may be used in targeted attacks, advertising campaigns, or similar. This is obviously subject to the caveat that the user may permit the capture of such data as part of any existing license agreement. Where this is the case, the license agreement must make it clear that information is to be recorded.

Financial Information:  VERIFIED


Personal Information:  VERIFIED



## OS Corruption

While a solution may be a genuine attempt at providing security to the user, errors in the solution may lead to the creation of vulnerabilities or the corruption of the host OS. No solution is perfect, but the installation of the solution under test must not be to the detriment of the host. Where vulnerabilities are discovered, the solution provider must be able to demonstrate that steps are taken to eliminate them. Corruption of the OS, in this case, is defined as the OS no longer operating or reporting critical failures directly related to the presence of the solution.

Vulnerabilities:  VERIFIED

Host Corruption:  VERIFIED

## 3rd Party Software/Adware


The installation of 3rd party applications, either as part of a partnership programme or to enable certain functions within the solution, are quite common. This section of the Verified scheme is intended to detect where those subsequent installations are malicious or otherwise lead to compromised security. The solution should also request consent from the user before any such installation.

Genuine Application:  VERIFIED

User Consent:  VERIFIED

## Removal

The installation of 3rd party applications, either as part of a partnership programme or to enable certain functions within the solution, are quite common. This section of the Verified scheme is intended to detect where those subsequent installations are malicious or otherwise lead to compromised security. The solution should also request consent from the user before any such installation.

Genuine Application:  VERIFIED

User Consent:  VERIFIED

## Disclaimer

While Checkmark Certified is dedicated to ensuring the highest standard of security product testing in the industry, it is never possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose. Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by Checkmark Certified should seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations. All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

Checkmark Certified provides test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.