Virus Bulletin

Covering the global threat landscape

VB100 TEST REPORT

Varist

Malware Detection Engine

September 21, 2026

Test result

Test passed

A

Detection grade

Grade A

Certification

98.71% malware detected

Clean

0.000% false alarms

Quick Summary

Product version

2.3.1

Test date:

September 1, 2026

Test methodology

VB100 1.7 Link

Test platform

Microsoft Windows 11 Pro, 64-bit, 10.0.26200

Executive summary

We tested **Malware Detection Engine** (version 2.3.1) on September 1, 2026, on Microsoft Windows 11 Pro, 64-bit, 10.0.26200, as per the 1.7 version of the VB100 methodology.

The tested product has successfully met the VB100 test criteria, with a malware detection grade of A.

Test criteria:

- The product must detect at least 75.00% of all test cases in the Certification set (malicious samples).
- The product must not generate more than 0.05% false alarms in the Clean set (legitimate program samples).

Where to find more details

For detailed test results, please consult the rest of the report. You may also find the links below useful for up-to-date information on how to interpret the report data.

- **Report reader's guide** Link
  Everything you find in this report, explained.
- **Testing methodology, version 1.7** Link
  Learn exactly how we test.
- **VB100 on the web** Link
  VB100 news and certified products.

AMTSO Standard Compliance

Virus Bulletin executed this test in accordance with the AMTSO Standard of the Anti-Malware Testing Standards Organization. The compliance status can be verified on the **AMTSO website**.

Test sets and product response

The VB100 test uses multiple sets of malicious and clean test cases to verify the ability of the tested product to detect malware, and to do so without generating false alarms for legitimate programs.

AT A GLANCE

CERTIFICATION	CLEAN
Description	**Description**
Common and prevalent Windows malware recently observed in the the wild.	A random selection of some widely and less widely used legitimate program files.
Type	**Type**
Outcome	**Outcome**
Pass	**Pass**
Detection rate	**False alarm rate**
98.71%	**0.000%**
Best possible outcome: **100.00%**	Best possible outcome: **0.00%**
Requirement: >= **75.00%**	Requirement: <= **0.05%**

DETAILED TEST RESULTS

Total cases tested	**Total cases tested**
1,857	**100,000**
Cases detected	**Cases with false alarm**
1,833	**0**
Cases missed	**Cases without false alarm**
24	**100,000**

TEST SET COMPOSITION

Windows PE executables	**Windows PE executables**
1,857	**30,805**
Other file types	**Other file types**
0	**69,195**

Report notes

Report notes contain complementary information that may be of interest to the report reader. Likewise, any extraordinary circumstance—particularly, those that may affect the test results—are recorded in these notes.

1. Unlike a standalone endpoint security solution, this product is a malware detection engine designed to be integrated with other technologies in real-world usage scenarios. This test simulated such integration by interacting with the engine's Scanserver component using a custom client developed by Virus Bulletin. The custom client submitted both malicious and clean files to the engine for scanning and performed remediation based on the engine's verdicts.

Virus Bulletin Ltd

Manor House, Howbery Business Park

Wallingford OX10 8BA, United Kingdom

+44 20 3920 6348

editorial@virusbulletin.com

https://www.virusbulletin.com/

Head of Testing: Péter Karsai

Security Test Engineers: Kitti Csia, Adrian Luca, Ionuţ Răileanu, Bálint Tanos

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin