Microsoft

Transparency report

Examining SE Labs test results, January-March 2020

Prepared by

Microsoft Defender ATP Research Team

Table of Contents

1 Summary of latest industry test results

This report provides a review of the latest independent industry test results for Microsoft Defender Antivirus (formerly Windows Defender Antivirus), the next-generation protection component of Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP), Microsoft's unified endpoint protection platform.

Over the last few years, Microsoft has been improving its performance in industry tests. Today, it consistently achieves high scores in these tests, demonstrating the strength of our protection capabilities and the innovations we continue to make in our security technologies.

While current antivirus tests don't necessarily reflect how attacks operate and how solutions are deployed in the real world, they can influence important business decisions. We are actively working with several leading industry testers to evolve security testing. Meanwhile, we're publishing this report to provide more details, insights, and context on test results. We'd like to be transparent to our customers and to the industry about our wins as well as improvement plans because of these tests.

1.1 SE Labs: AAA Award (January–March 2020)

In SE Labs' Enterprise Endpoint Protection test for January-March 2020 (Q1), Microsoft Defender Antivirus won the AAA Award.

Microsoft Defender Antivirus registered 96% Protection Accuracy rating and 97% Legitimate Accuracy rating in January–March 2020 test periods for a consistent Total Accuracy rating of 97%. Learn More >>

2 Examining the SE Labs results

2.1 Summary of overall results

The table below summarizes the overall test results for Microsoft Defender Antivirus in the January-March 2020 testing by SE Labs:

Test category	Jan-Mar
Protection Accuracy	96%
Web downloads score	74/75
Targeted attacks score	25/25
Legitimate software accuracy	97%
Total accuracy rating	**97%**

Table 1. Overall Microsoft Defender Antivirus test results in the SE Labs test.

2.2 Understanding Protection Accuracy test scores

SE Labs determines the Protection Accuracy scores based on the combined outcome of two tests:

1. Web downloads (74 test cases)
2. Targeted attacks (25 test cases)

SE Labs goes beyond the binary rating (i.e., blocked vs. compromised) in rating protection effectiveness. Instead, SE Labs considers the nuances of the interaction between the product and the threat. For example, it issues a different rating for *Blocked (+2 points)* from what is given for *Complete remediation (+1 points)* or a *Compromised system (-5 points)*. The other ratings used by SE Labs for both Web downloads and Targeted attacks tests are: *Detected (+1)*, *Neutralized (+1)*, *Persistent neutralization (-2)*. A rating is assigned to each product-threat interaction operation and a combined score is calculated for each product.

Microsoft Defender Antivirus achieved the following combined score for web downloads and the targeted attack tests.

	Jan-Mar
Detected	99
Blocked	95
Neutralized	4
Compromised	1
Protected	99

Table 2. Summary of Microsoft Defender Antivirus scores in the Protection Accuracy test

In the January-March 2020 test, Microsoft Defender Antivirus missed 1 of the 74 samples used in the web downloads test.

When it comes to the targeted attacks test, the protection score considers the extent of protection demonstrated by the product (i.e., the attack stage in which the product was able to block the threat). Points are deducted for *Access (-1)*, *Action (-1)*, *Escalation (-2)*, and *Post-escalation action (-1)*.

2.3 Understanding Legitimate Software Accuracy test scores

SE Labs Legitimate Software Accuracy test measures the endpoint product's ability to correctly classify legitimate applications. SE Labs assigns ratings based on how the product classifies an object (safe, unknown, not classified, suspicious, unwanted, or malicious) and the level of interaction required of the user (e.g., click, or no interaction required).

SE Labs also takes into consideration the prevalence of the legitimate application to account for the breadth of the business impact of incorrectly blocking. This prevalence factor is expressed as a modifier and is multiplied by the interaction rating to determine the product score.

Microsoft Defender Antivirus correctly classified 97% of legitimate applications as safe in January-March 2020 test cycle.

2.3.1 Analysis: What kinds of files were misclassified?

Our research team analyzed the sample that Microsoft Defender Antivirus misclassified and assigned proper determination. The team also analyzed the root cause of these misclassifications and worked with threat research teams to enhance detection accuracy.

Below are the two files that Microsoft Defender Antivirus misclassified in the test cycle.

Sample	Description	Digitally signed? (Y/N)
Sample 1	Game application software	Y
Sample 2	Game player application	Y