

# Transparency report

## Examining the AV-TEST September-October 2018 results

*Prepared by*

Windows Defender Research Team

© 2019 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

The descriptions of other companies' products in this document, if any, are provided solely as a convenience to aid understanding and should not be considered authoritative or an endorsement by Microsoft. For authoritative descriptions of any non-Microsoft products described herein, please consult the products' respective manufacturers.

Any use or distribution of these materials without the express authorization of Microsoft is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft in the United States and/or other countries.

# Table of Contents

1	Introduction .....	2
1.1	Key takeaways.....	2
2	Examining test results.....	3
2.1	Summary of overall scores.....	3
2.2	Understanding Protection scores.....	3
2.2.1	True Real-World Testing: Running against the unified Windows Defender ATP protection platform....	5
2.2.2	We took notice: Improvements based on False Negatives.....	6
2.3	Understanding Usability scores.....	7
2.3.1	Analysis: What kinds of files were misclassified? .....	7
2.3.2	The synthetic nature of usability tests.....	7
2.3.3	Criteria for classifying files may vary across vendors and testers.....	8
2.3.4	We took notice: How the Windows Defender Antivirus team dealt with FPs.....	9
2.4	Understanding Performance scores.....	9

# 1 Introduction

In [AV-TEST's September-October 2018](#) testing cycle, [Windows Defender Antivirus](#) achieved perfect scores (6.0/6.0) in the Protection and Usability test modules and a score of 5.0/6.0 in the Performance module. This report presents more details on test scores, with commentary for context and transparency.

## 1.1 Key takeaways

Below is a summary of the key takeaways from this report:



### **Protection**

Windows Defender Antivirus maintained an overall Protection score of 6.0/6.0, protecting against 21,566 of 21,568 tested malware samples. [Learn more](#)



### **Usability (false positives)**

Windows Defender Antivirus also maintained a Usability score of 6.0/6.0 after misclassifying only 1 out of 1,342,277 tested files. [Learn more](#)



### **Performance**

Windows Defender Antivirus achieved an overall Performance score of 5.0/6.0, a decrease from its previous 6.0/6.0 score. Windows Defender Antivirus showed higher performance impact in low frequency actions (e.g., software installation). [Learn more](#)



### **Testing methodology**

Microsoft continues to observe areas to improve alignment between testing methodologies and the way threats occur in the real world. Microsoft is working with a number of testers to bridge the gap and drive true real-world testing.

## 2 Examining test results

### 2.1 Summary of overall scores

The table below summarizes the overall test results for Windows Defender Antivirus in the September-October 2018 antivirus testing by AV-TEST:

	Protection	Usability	Performance
Overall scores for this cycle >>>	6.0/6.0 ( $\pm 0$ )	6.0/6.0 ( $\pm 0$ )	5.0/6.0 (-1.0)

Table 1. Windows Defender Antivirus' overall antivirus test results in the [September-October 2018 AV-TEST Business User test](#). AV-TEST uses [Protection](#), and [Usability](#), and [Performance](#) test modules.

### 2.2 Understanding Protection scores

Below are details on the Protection test scores:

	Sept	October
"Real World" testing	100% (169/169)	99.3% (141/142)
"Prevalent malware" testing	100% (11,856/11,856)	99.99% (9,400/9,401)
Overall malware protection rate (all samples)	100% (21,566/ 21,568)	
Overall Protection score for this cycle >>>	<b>6.0/6.0 (<math>\pm 0</math>)</b>	
Overall Protection ranking for this cycle >>	1 <sup>st</sup> out of 18 (tied with 11 more)	

Table 2. Summary of [Protection](#) scores for the Sept-October 2018 Business User test

The diagrams below show Windows Defender Antivirus detection rates in "Prevalent malware" and "Real World" testing over a one-year period:

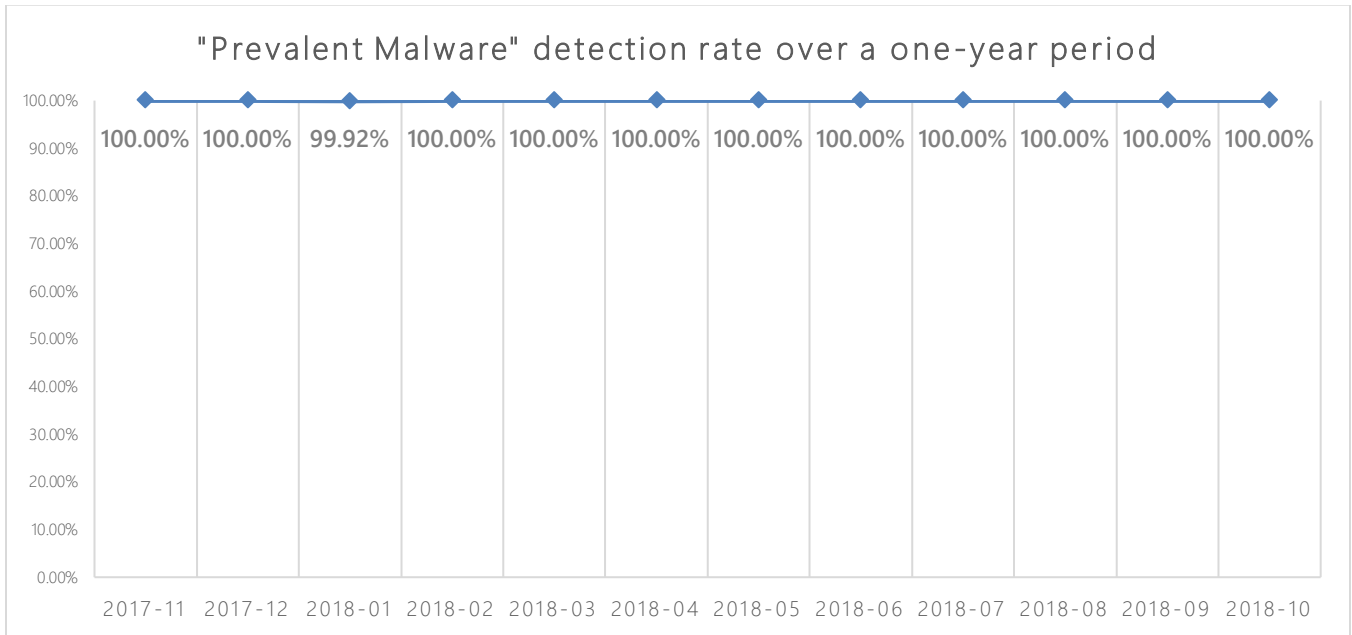


Figure 1. Windows Defender Antivirus detection rates in AV-TEST "Prevalent malware" tests over a one-year period

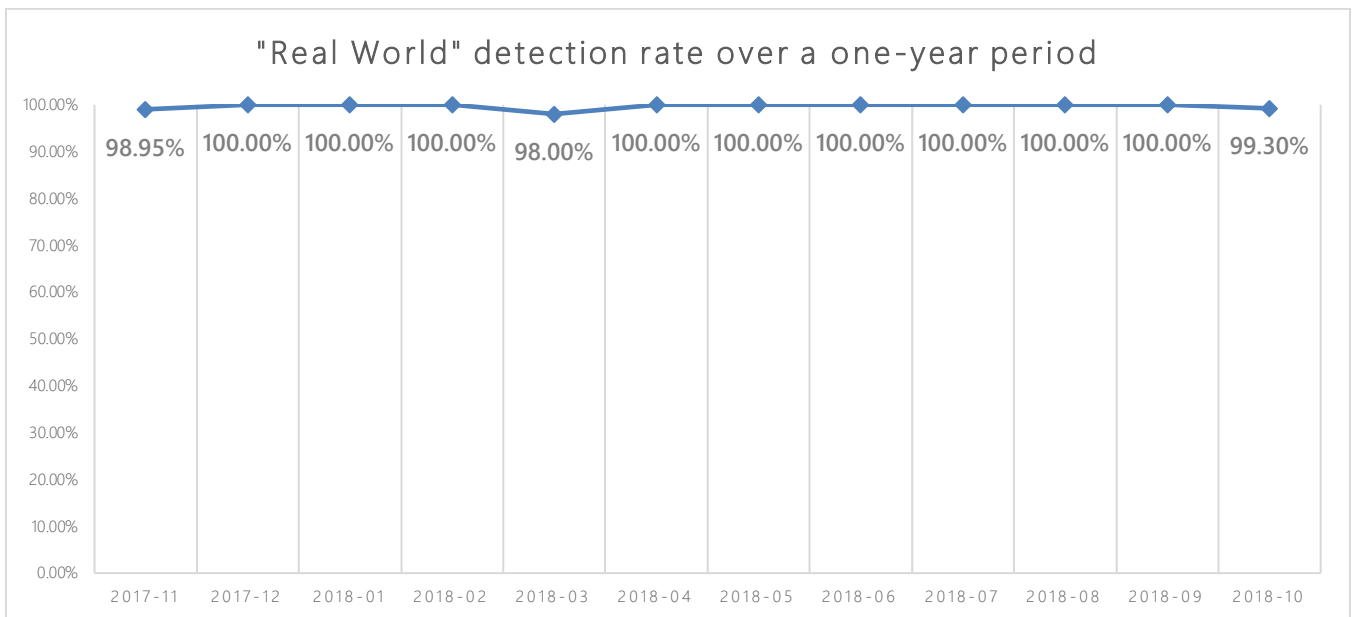


Figure 2. Windows Defender Antivirus detection rates in AV-TEST "Real World" tests over a one-year period

## 2.2.1 True real-world testing: Running against the unified Windows Defender ATP protection platform

The Windows Defender Research team tested the two missed samples against the Windows Defender ATP stack to assess the missed samples' ability to infect a machine in a real-world enterprise environment. This expands on the testing practice that isolates AV from the rest of the environment. As expected, the malware samples were blocked and detected by several stack components, as follows:

### Sample 1

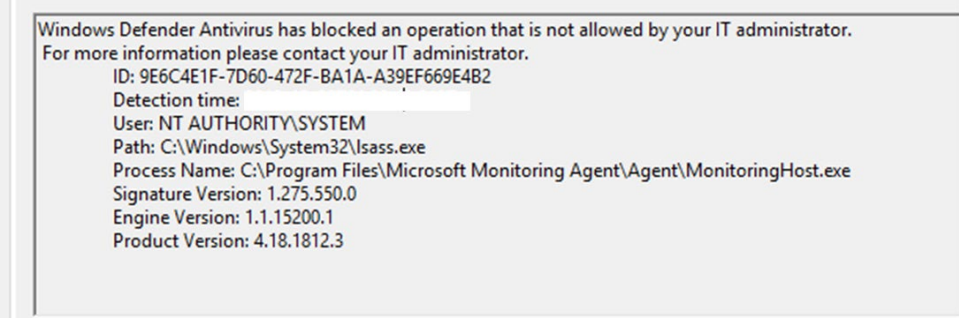
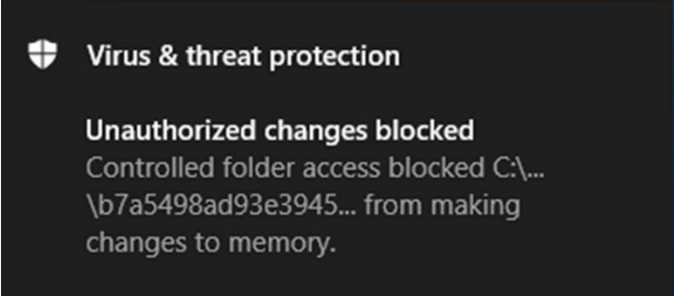
Windows Defender ATP component	Outcome
Attack surface reduction	<p>File blocked by the Attack surface reduction rule "Block credential stealing from the Windows local security authority subsystem (lsass.exe)"</p> 
Controlled folder access	<p>File blocked by Controlled folder access (Untrusted file attempting to make changes to sensitive memory location):</p> 
Application control	<p>File blocked from running under the following modes:</p> <ul style="list-style-type: none"> <li>- Whitelisting mode</li> <li>- Managed Installer mode</li> </ul>
Hardware-based isolation	<p>File blocked from being downloaded and run from the web when Windows Defender Application Guard is enabled</p>

Table 1 Running sample 1 against the Windows Defender ATP stack

## Sample 2

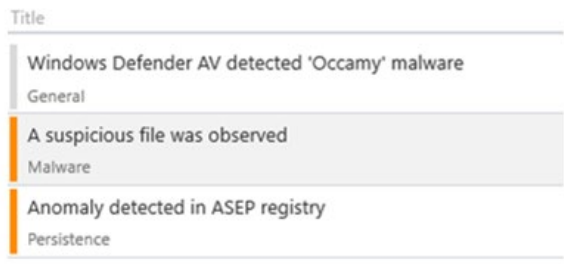
Windows Defender ATP component	Outcome
Endpoint detection and response (EDR)	<p>File triggered several alerts</p> <p>Alerts related to this file</p> 
Application control	<p>File blocked from running under the following modes:</p> <ul style="list-style-type: none"> <li>- Whitelisting mode</li> <li>- Managed Installer mode</li> </ul>
Hardware-based isolation	File blocked from being downloaded and run from the web when Windows Defender Application Guard is enabled

Table 2 Running sample 2 against the Windows Defender ATP stack

### 2.2.2 We took notice: Improvements based on false negatives

Despite having a perfect score in the “Protection” test, Windows Defender AV missed 2 out of 21,568 tested samples. We take those misses as a learning opportunity to improve our product and protection quality. The table below shows the two samples missed, and the improvements that were made as a result:

Missed File	Root cause	Improvements
File 1	Incorrect “clean” determination	<ul style="list-style-type: none"> <li>• Improved heuristics for differentiating legitimate network drivers (e.g., ones that monitor bandwidth) from malicious network drivers (e.g., ones that exfiltrate traffic)</li> <li>• Implemented process improvements that included automatic flagging of potentially incorrect determinations that may cause false allows so they can be reviewed and validated</li> </ul>
File 2	No classification	<ul style="list-style-type: none"> <li>• Enhanced generic classifiers/detections for malware that use multi-layered evasion techniques</li> </ul>

Table 3 Resulting improvements



## 2.3 Understanding Usability scores

In Usability tests, AV-TEST includes clean file samples in the test population and checks whether antivirus products incorrectly classify them as malware (what is known as false positive, or FP). Below is a summary of results in the Usability test:

	September	October
Number of misclassified files	1 (out of 664,426 samples)	0 (out of 677,581 samples)
Overall Usability score for this cycle >>>	<b>6.0/6.0 (±0)</b>	
Overall Usability ranking for this cycle >>>	1 <sup>st</sup> out of 18 (tied with 12 more)	

Table 3. Summary of [Usability test](#) scores for the September-October 2018 Business User test

### 2.3.1 Analysis: What kinds of files were misclassified?

Below is a description of the file that Windows Defender Antivirus misclassified in this test cycle. Based on our research and file prevalence data, the misclassified sample is not common in enterprise environments.

Sample	File prevalence (30 days)	Description	Digitally signed? (Y/N)
Sample a	13	Optical design software	No

Table 4. Files that Windows Defender antivirus incorrectly classified as malware

Microsoft encourages software vendors to take [steps to raise the level of trust](#) both by security vendors and users alike. These steps include signing software with certificates issued by reputable Certification Authorities.

### 2.3.2 The synthetic nature of usability tests

Misclassifications in a synthetic test are not necessarily indicative of false positives in real-world scenarios. This is true because the current test methodology discounts contextual elements that Windows Defender Antivirus uses for issuing a verdict on a file. For example, when a file is tested, it is not downloaded from the vendor website. Both the original file name and the download site are contextual information that are removed in tests. We've seen many cases where a customer in the real world downloads a clean program from the vendor site without encountering any erroneous detection. However, when a tester gives the file a seemingly random name (e.g., its SHA-256 hash), removes the mark of the web, and doesn't download the file from the vendor website, some of our more aggressive machine learning models issue blocks that don't occur in the real world.

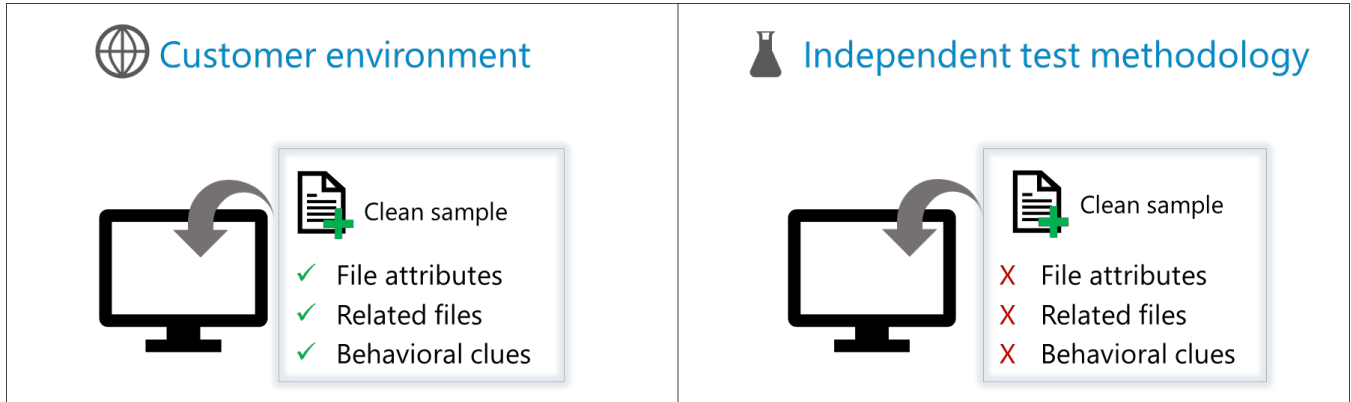


Figure 3. In some cases, samples are incorrectly classified (false positive) in the synthetic test environment but not on customer machines.

### 2.3.3 Criteria for classifying files may vary across vendors and testers

The criteria for classification can vary between antivirus vendors and testers depending on their policies. Some files identified as clean by some vendors could be files that Windows Defender Antivirus identifies as potentially unwanted application (PUA) and thus would be blocked. Microsoft’s policy aims to protect customers against malicious software while minimizing the restrictions on developers. The diagram below demonstrates the high-level [evaluation criteria](#) Microsoft uses for classifying samples:

- Malicious software: Performs malicious actions on a computer.
- Unwanted software: Exhibits the behavior of adware, browser modifier, misleading, monitoring tool, or software bundler
- Potentially unwanted application (PUA): Exhibits behaviors that degrade the Windows experience
- Clean: We trust that the file is not malicious, is not inappropriate for an enterprise environment, and does not degrade the Windows experience

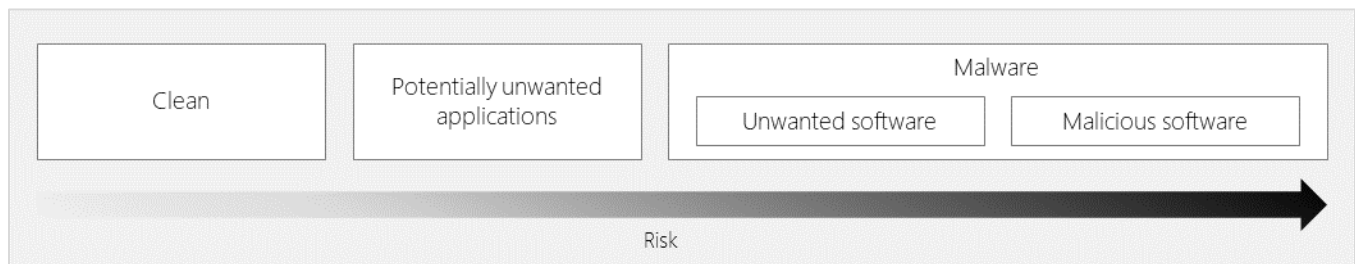


Figure 4. Microsoft's high-level sample classification criteria

### 2.3.4 We took notice: How the Windows Defender Antivirus team dealt with FPs

Our research team analyzed the sample that Windows Defender AV misclassified and assigned a proper determination. The team also analyzed the root cause for the misclassification and retrained some of our machine learning modules to avoid similar misclassifications in the future.

## 2.4 Understanding Performance scores

Performance tests measure the effect of certain user actions, which are executed as part of the test, on system speed. The table below summarizes Performance test results in the September-October cycle:

Sept-October	
Performance test score for this cycle	5.0/6.0 (-1.0)
Performance ranking for this cycle	3 <sup>rd</sup> out of 16 (tied with 4 more vendors)

Table 5. [Performance test](#) results for Windows Defender Antivirus for the Sept-October cycle

The table below presents the details of performance test results compared to industry averages. Performance is measured by the average impact of the product on computer speed. Therefore, a smaller number is favorable. Green boxes indicate areas where Windows Defender Antivirus performed better than the industry average; orange boxes indicate areas lower than the industry average.

Action	Standard PC	Industry average	High End PC	Industry average
Launching popular websites	7%	12%	7%	11%
Downloading frequently-used applications*	3%	1%	1%	1%
Launching standard software applications	14%	13%	12%	11%
Installation of frequently-used applications	85%	31%	51%	31%
Copying of files (locally and in a network)	1%	5%	1%	6%

Table 4. Average impact of the product on computer speed in daily usage

\*The description for these operations is given by AV-TEST and might not be aligned with what Microsoft's data indicates as realistic.

Based on results presented in the table above, Windows Defender Antivirus performed better than the industry average in several areas. For the areas where it underperformed, the largest gap between Windows Defender Antivirus' performance and the industry average is in the area that AV-TEST labels as *Installation of frequently-used applications*. There are several factors to consider for driving the right conclusion out of these test results:

- **Consider the frequency of the action**

Most users in enterprise environments are information workers whose common user activities include:

- Browsing the web
- Using email clients
- Processing documents
- Accessing network resources

Users spend substantially less time installing new applications compared to the activities listed above. This is true for all user segments, but especially for enterprises, where software installation is usually governed by usage policies. Windows Defender Antivirus is optimized for delivering high levels of performance during high-frequency actions. For example, *Installation of frequently used applications* (a low-frequency action) is the area where Windows Defender Antivirus scored substantially lower than the industry average. Performance is a priority area for the Windows Defender Antivirus team, and we're working to improve it even further.

- **Consider the level of risk**

Windows Defender Antivirus is designed to perform thorough scanning during the software installation process. This could have a performance cost. One reason for this is that software installation is a relatively complex operation that touches different areas of the operating system. Thorough inspection is necessary to reduce the risk of introducing malicious software on the system.

- **What impactful areas are not being tested?**

There are several areas that are not being tested for performance by AV-TEST that are critical to user experience. Examples include:

- Shutdown and startup
- Universal Windows app launch
- Battery consumption