AV-TEST
CYBERSECURITY FOUNDATION

Product of the Year 2026*

Recommended security solutions
for Windows 10-11 & Windows Server

amtso
The cybersecurity industry's testing standard community
STANDARD

MVI
Microsoft Virus Initiative
MVI-Compliant Testing Methodology

*Based on the 2025 Advanced In-The-Wild Malware Test results

FEBRUARY 2026

Table of contents

Advanced In-The-Wild Malware Test – **Summary 2025**

The purpose of the Advanced In-The-Wild Malware Test 2025 is to identify security vendors whose solutions meet the rigorous testing requirements defined by the AVLab Cybersecurity Foundation. The “Product of the Year 2026” and “TOP Remediation Time 2026” certificates are awarded based on the results of multi-stage tests conducted in conditions that closely reflect real-world user environments.

The “Product of the Year 2026” certificate is granted to solutions that deliver comprehensive protection for Windows and Windows Server systems. The assessment covers the entire attack chain, with particular emphasis on realistic usage scenarios, including interaction with web content, downloading files from untrusted sources, and executing them within the operating system.

The second award, “TOP Remediation Time 2026,” focuses on the speed and effectiveness of the response after malware execution. The analysis evaluates the product’s ability to interrupt malicious activity, remove threat components, and restore the system to a secure state. Mechanisms such as automatic neutralization, operating system restart, rollback, and automated data recovery are taken into account.

The Advanced In-The-Wild Malware Test series is characterized by a high level of methodological precision. The tests use real in-the-wild malware samples delivered via common attack vectors, including websites and user-initiated downloads. The objective is to evaluate product behavior under realistic exposure to active, real-world threats.

All tested solutions are evaluated using the manufacturer’s default configuration or, where justified, with additional protection features enabled. Any deviation from the default setup is clearly documented and described in the test report after each edition, ensuring full transparency and repeatability of the results.

amtso
The cybersecurity industry's testing standard community
STANDARD

MVI
Microsoft Virus Initiative

The Advanced In-The-Wild Malware Test is conducted in accordance with AMTSO testing guidelines and complies with Microsoft Virus Initiative requirements.

II Criteria for **Awarding Certificates**

To obtain the Product of the Year 2026 certificate, a tested solution was required to meet the following conditions:

Participate in at least three editions of the Advanced In-The-Wild Malware Test (six editions are conducted annually).
Achieve the EXCELLENT certification in all three editions, corresponding to a minimum 99% protection effectiveness* in each test.

To obtain the additional TOP Remediation Time 2026 certificate, the tested solution was required to meet the following condition:

Successfully neutralize 100% of threats in at least three test editions. If the solution was evaluated in more than three editions, the three editions with the highest average Remediation Time performance (i.e., the lowest average Remediation Time values) were taken into account for the final assessment.

*From 2026, we are raising the threshold from 99% to 99.6%, and in the linked article we explain why we are doing this: https://avlab.pl/en/we-are-changing-the-certification-thresholds-in-the-advanced-in-the-wild-malware-test/

What Are These Tests? – **Key Information**

The Advanced In-The-Wild Malware Test is a long-term research initiative designed to evaluate the effectiveness of security solutions in protecting against malware under real-world conditions. The test focuses both on a product's ability to prevent infections at the threat delivery stage (Web-Layer, Pre-Launch) and on its capability to detect and neutralize attacks after malicious code has been executed in the system (Runtime Defense, Post-Launch). The assessment includes business-grade security solutions, often equipped with advanced EDR/XDR mechanisms, as well as products intended for individual users.

In practice, the test recreates realistic user behavior on a Windows system while browsing the internet, which reflects the most common infection vector. In this scenario, the user may fall victim to social engineering techniques and unknowingly download and execute malicious software, thereby initiating an attack in the Runtime environment.

The test uses real in-the-wild malware samples obtained from active URLs, ensuring a high level of realism and practical relevance for both end users and security vendors. After each edition, detailed technical data are published, covering the effectiveness of threat blocking at the Web-Layer stage, protection response in Runtime, and the time required to detect and neutralize an active attack (Remediation Time). Conducted in a graphical Windows environment, the test also evaluates the ability of products to automatically remediate incidents and restore the system to a secure state after an attack.

IV Three-Step Analysis **Methodology**

1. Malware Selection Algorithm
2. Simulating a Realistic System Protection Scenario
3. Incident Remediation Time Assessment

The test results are based on three consecutive procedures, the first of which involves the selection of malware samples and the analysis of related events and telemetry logs.

Malware samples are continuously collected in the form of active, real-world URLs available on the internet. The samples originate from multiple sources, including public threat intelligence feeds, honeypots, and both closed and open groups on the Telegram messaging platform. This approach allows for the creation of a current and diverse set of real-world threats.

Before being used in the test, each malware sample undergoes a multi-stage technical verification process. One of the key steps involves comparing the SHA-256 checksum against an existing database, which eliminates the risk of re-testing previously analyzed malware.

Subsequently, the samples are analyzed in a Windows environment using hundreds of detection rules based on commonly observed attack techniques, including LOLBins mechanisms. System processes, network communication, Windows registry changes, and other system modifications are closely monitored in order to clearly determine which behaviors confirm the malicious nature of each sample.

1 Malware Selection **Algorithm**

Each potentially malicious file is evaluated according to the following algorithm:

A POTENTIALLY MALICIOUS FILE

VALIDATION AND ANALYSIS WORKFLOW

1. **Is the file available online?**
   The threat must be accessible online and available for download.
2. **Is the file unique?**
   The file's SHA-256 hash is compared against an internal database to eliminate duplicates.
3. **Is the file suitable for testing?**
   The original Windows file extension is verified to ensure relevance to the test scope.
4. **Static analysis**
   The sample is analyzed using YARA rules and a technology partner's malware scanner to
5. **Dynamic analysis**
   The file is executed in a Windows 11 environment to determine whether it exhibits malicious behavior.

MALWARE SELECTED FOR TESTING

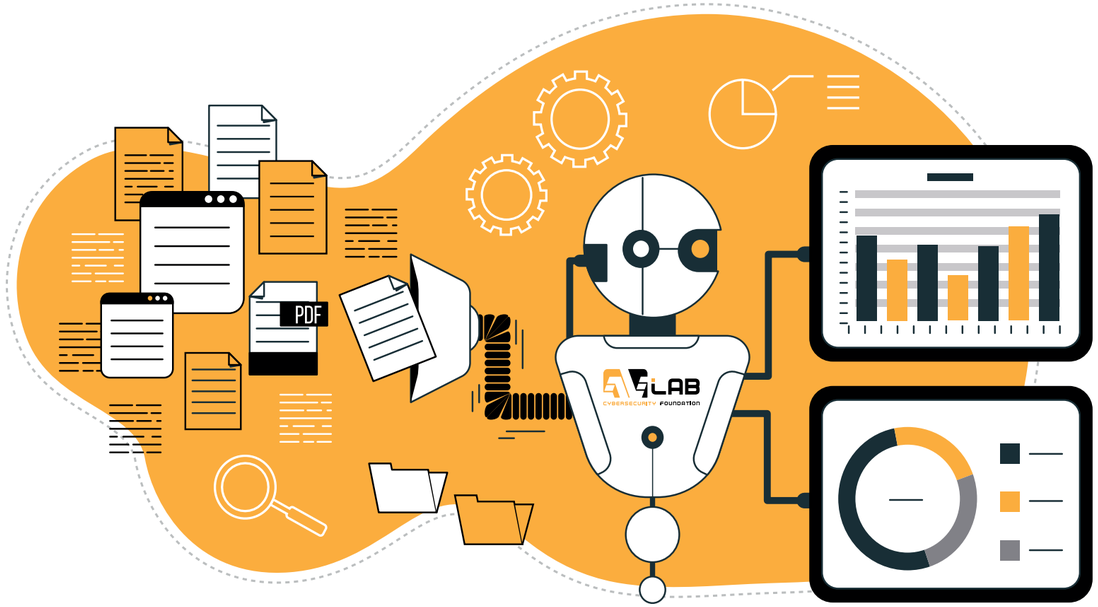
NO MALICIOUS ACTIVITY OBSERVED
(sample rejected)

✱ Many threats used in the test are distributed over the HTTPS protocol, which is often abused to create a false sense of trust. Attackers can easily deploy SSL/TLS certificates, and some malicious files are hosted on legitimate web servers whose reputation is leveraged to bypass basic security controls and more effectively deliver malware.

2 Simulating a Realistic **System Protection Scenario**

At this stage, each confirmed malware sample is simultaneously downloaded via a web browser from its original URL to Windows systems on which the tested security solutions are installed, representing the Web-Layer (Pre-Launch) phase of the attack. All products are exposed to the same threat at the same time, ensuring equal and comparable testing conditions.

The test reflects a realistic infection scenario in which the threat is delivered to the system through a web browser and a file download from an active URL—for example, from a compromised or malicious website, or via a link delivered through a messaging application, an email message, or a document. The link is opened in the Opera browser, allowing the test to accurately reproduce typical end-user behavior and real-world operating conditions.



The result for each malware sample **is classified into one of the following levels:**

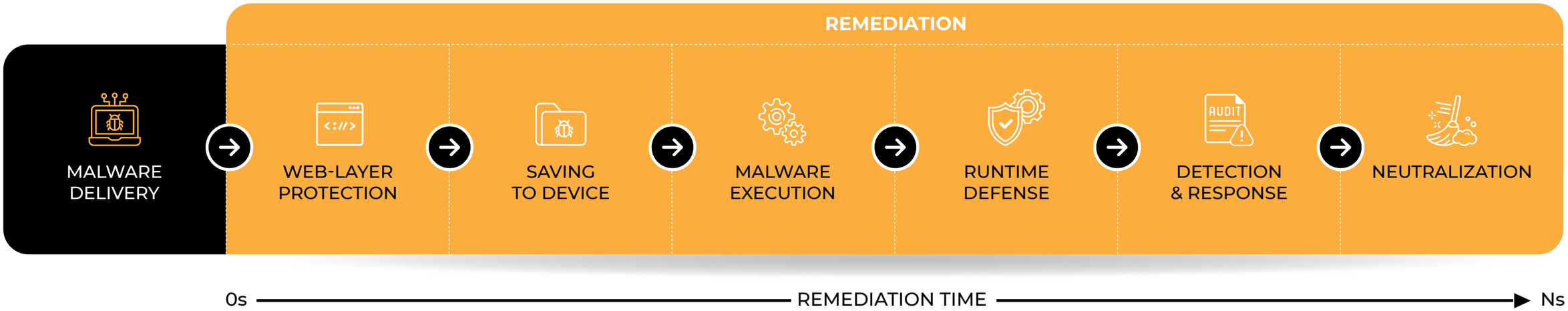
A Pre-Launch (Web-Layer Protection) result is assigned when the link leading to a malicious file is blocked at the browser level or when the file is automatically removed immediately after being saved to disk. This indicates that the threat was stopped at the delivery stage, before any malicious code was executed within the operating system. This stage reflects prevention at the web layer, prior to the actual execution of malware.

A Post-Launch (Runtime Defense) result is assigned when malware is successfully downloaded and executed, but its malicious activity is detected and neutralized during runtime. This level represents the product's effectiveness in protecting the system against active threats, including zero-day attacks. It applies to threats identified after execution, regardless of whether detection and response occur locally or via cloud-based technologies. At this stage, protection depends on the solution's ability to perform multi-layer behavioral analysis, correlate events, and rapidly neutralize an ongoing attack.

A System Compromised (Fail) result is assigned when malware is able to execute and continue its activity without being effectively detected or neutralized, leading to a successful compromise of the operating system. This includes scenarios where persistent changes are made to the system, sensitive data is exposed, or long-term communication with command-and-control infrastructure is established. This outcome indicates that the tested solution failed to prevent, detect, or adequately respond to the threat within the evaluated timeframe.

3 Incident Remediation **Time Assessment**

Subsequently, based on the collected telemetry logs, in addition to evaluating the effectiveness of detecting and blocking zero-day threats, the time required for the automatic neutralization of an active attack and remediation of incident impact is analyzed for each malware sample in the Runtime environment. This metric is referred to as Automatic Average Remediation Time and is calculated using the actual response time of the product from the moment the threat is executed to the effective neutralization of the attack and restoration of the system to a secure state. The tested solutions are configured so that the removal of attack artifacts and system remediation are performed fully automatically, without requiring any user interaction or decision. This approach enables an objective assessment of the product's real ability to autonomously respond to a security incident, which constitutes one of the key objectives of the test.



To estimate the Average Remediation Time, a security incident is assumed to begin at the moment a malware sample is delivered to the system via a file download from an active URL (Web-Layer). The threat is then executed in the test environment, and its activity is monitored during the Runtime phase over a dynamic analysis window lasting 7 to 9 minutes. If no response from the tested security product, such as detection, blocking, or remediation actions, is recorded within this time window, the analysis for the given sample concludes with a FAIL (System Compromise) result, indicating a successful compromise of the system. For samples in which the security product performs protective actions, the time required to detect Indicators of Compromise (IoCs) and to automatically neutralize the threat and restore the system to a secure state is measured from the moment of malware execution. The resulting time values form the basis for calculating the Average Remediation Time for the tested edition.

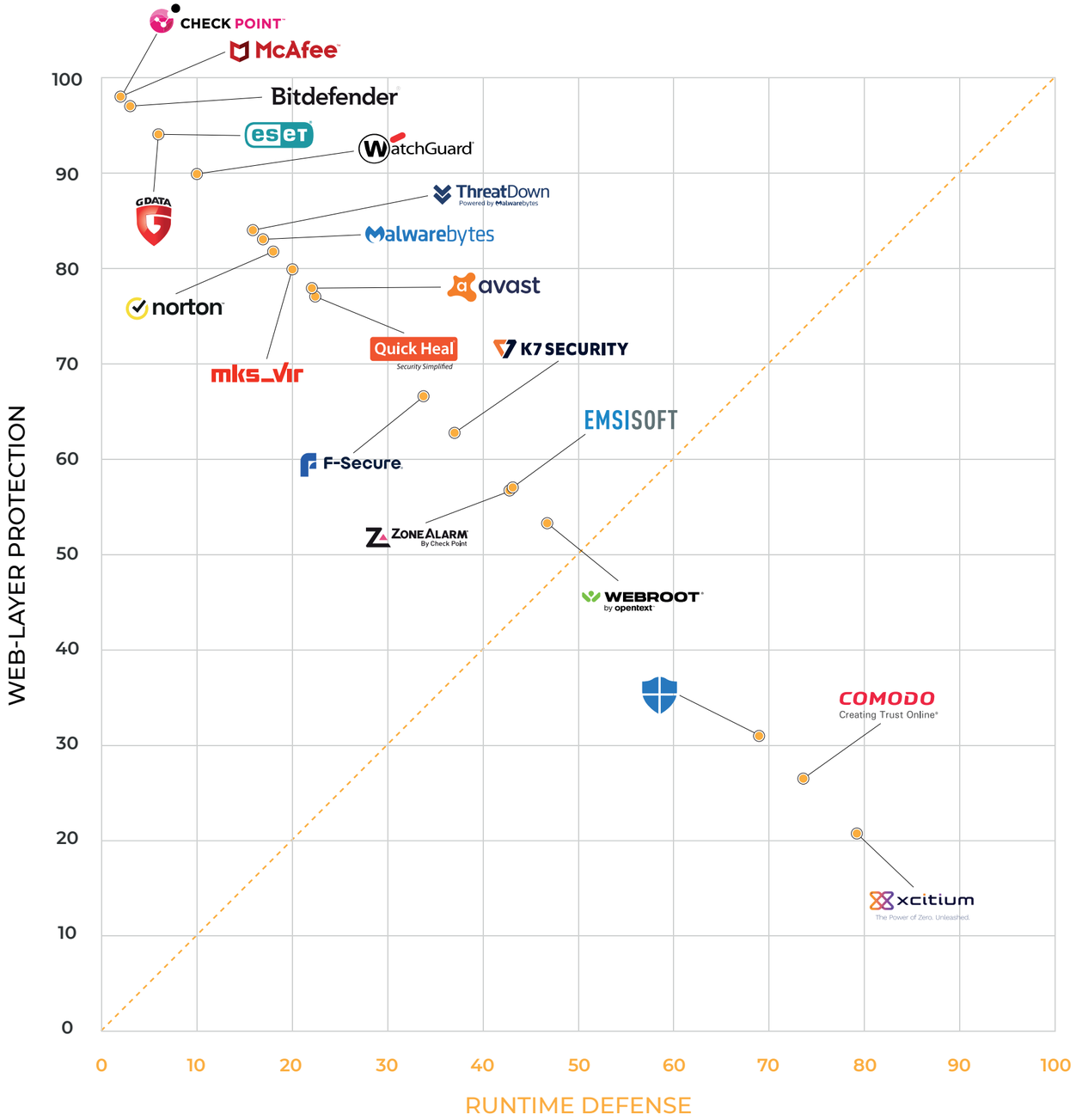
V Protection Effectiveness **Matrix**

The graphical placement of individual solutions in the Protection Effectiveness Matrix was developed based on the results achieved in combating malware used in the Advanced In-The-Wild Malware Test, taking into account only those solutions that participated in at least three editions of the test during the year.

The vertical axis reflects the effectiveness of early detection and blocking of threats at the delivery stage, i.e., before the malicious code is launched on the system (Web-Layer Protection, Pre-Launch).

The horizontal axis shows the ability to detect and neutralize threats after the file has been launched in the operating system (Runtime Defense, Post-Launch).

The position of the solution relative to the diagonal line indicates the dominant style of response to threats, i.e., the preference for protection at the Web-Layer stage or the effectiveness of actions taken in the Runtime Defense phase. This classification is based on a long-term analysis of thousands of real malware samples tested throughout the year.

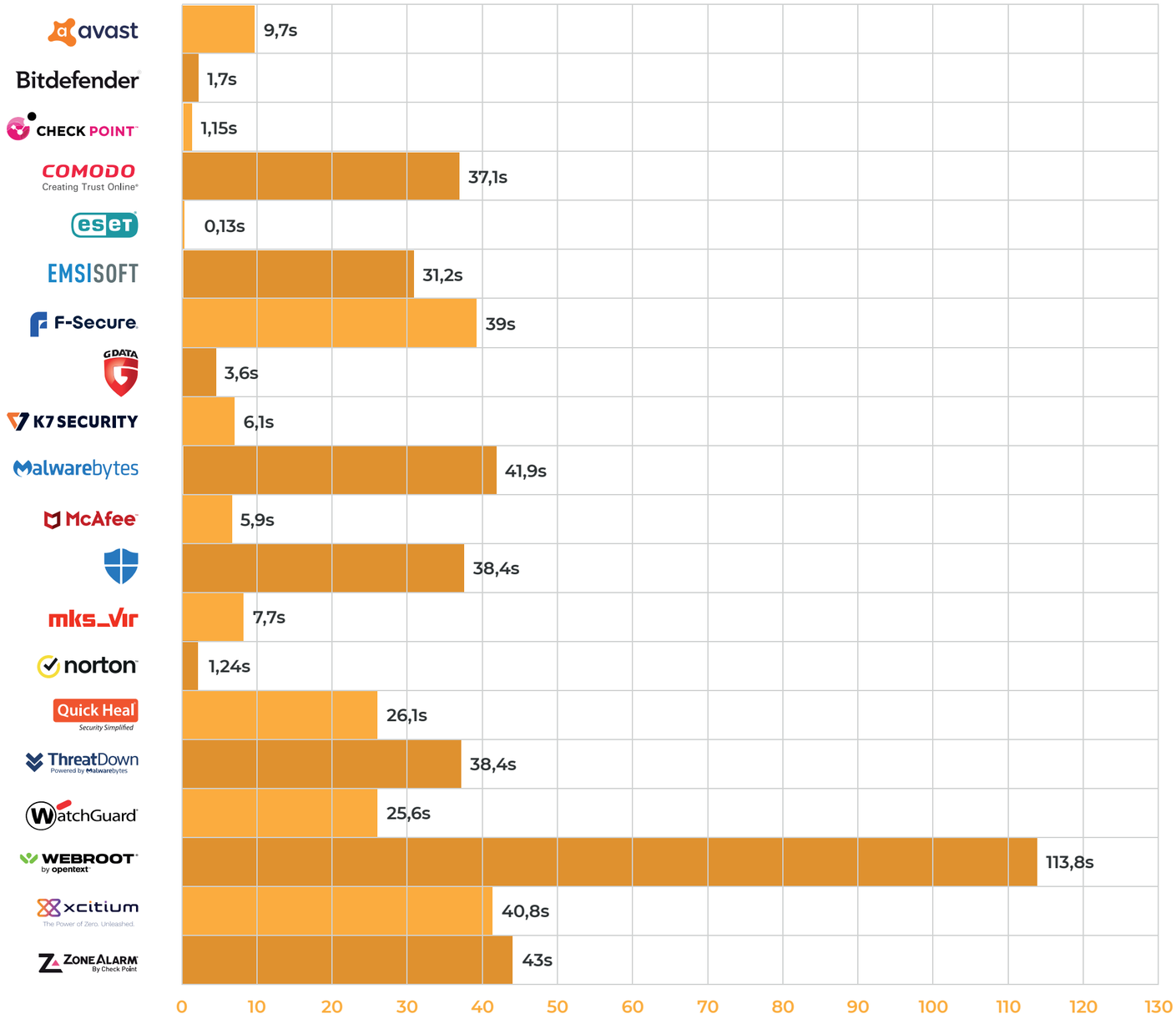


VI Average Remediation Time – **Annual Average Statistics**

The Remediation Time (RT) metric is used to determine the time required to detect and effectively neutralize a threat. It is calculated from the moment the malware sample is delivered to the system (Web-Layer Protection: detection, file download or save, and response) until the end of the Runtime Defense phase. This means that the malware can be executed and then subjected to advanced detection and security incident remediation mechanisms.

Remediation Time covers the full range of responses by the protection solution, including blocking access to the file, moving it to quarantine, analyzing it in a sandbox, removing the malicious code, reversing the changes made, and restoring the system to a secure state (Neutralization). For each test edition, the average Remediation Time is calculated based on all malware samples used, which allows for the development of comparable statistics between the tested solutions.

Incident remediation time is expressed in seconds and may vary depending on the security solution configuration, the manufacturer's architecture and infrastructure, as well as other technical factors.



VII Statistical data **from tests in 2025**

Based on feedback from files scanned using the engine of our technology partner, mks_vir sp. z o.o.

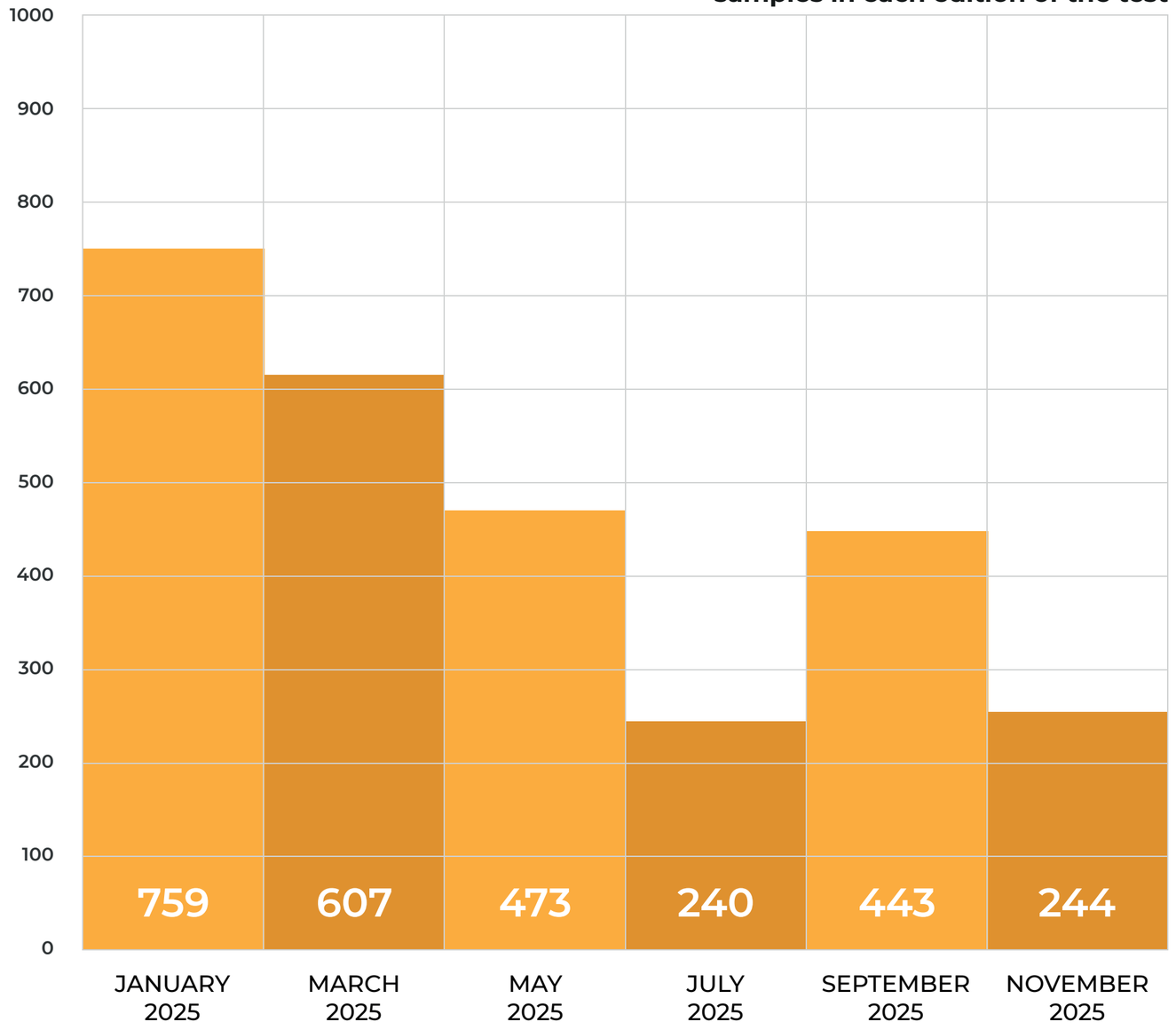
Basic information about malware

Taking into account telemetry data from the tested solutions, it was determined that in 2025, a total of 2,766 samples of unique, confirmed malware were used. Approximately 27% of them were blocked only at the Runtime Defense stage, i.e., after delivery to the system, at launch, or as a result of dynamic code analysis in the system environment. This is the highest-risk scenario, which clearly shows the importance of effective, multi-layered protection against modern threats.

Other information about the 2025 tests

- 6 editions of testing
- 2766 unique malware samples
- 73% level of Web-Layer Protection malware detection
- 27% level of Runtime Defense malware blocking
- 26s average Remediation Time for incident resolution

Total number of confirmed unique malware samples in each edition of the test



VIII Security solutions **tested in 2025**

Acronis
AURA
avast
Bitdefender
CHECK POINT
CISCO
COMODO Creating Trust Online®
EMSISOFT
eset
F-Secure
G DATA
K7 SECURITY
kaspersky
Malwarebytes
McAfee
mks_vir
norton
panda
Quick Heal Security Simplified
ThreatDown Powered by Malwarebytes
TREND MICRO
WatchGuard
WEBROOT by opentext
xcitium The Power of Zero. Unleashed.
ZoneAlarm By Check Point

This is not a complete list, as some manufacturers participate in testing anonymously in order to improve their security technologies. Companies that are interested in testing their solutions, obtaining certification, and would like to learn how to improve their software are welcome to contact us.

Below are the cards for manufacturers who have achieved Product of the Year or TOP Remediated Time certification in AVLab tests

Avast

Free Antivirus

Workstation protection software participated in all editions of the test.
In total, it blocked 2,766 real malware samples throughout the year.
This gives a maximum score of 100% of all in-the-wild threats neutralized.

- Over 67% of threats were blocked in the browser or immediately after being saved to disk without the malware being launched.
- Over 32% of malware samples were blocked after launch.
- Taking into account the three best results, Avast software needed an average of 9.7 seconds to automatically and flawlessly repair security

Based on the telemetry data obtained, we confirm that AVAST Free Antivirus did not once expose the operating system or the data on the disk to a potential leak as a result of running malware.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	55,99	44,01	-	100%	17,9	759
MARCH	55,52	44,48	-	100%	13,8	607
MAY	68,71	31,29	-	100%	12,0	473
JULY	92,08	7,92	-	100%	3,8	240
SEPTEMBER	96,61	3,39	-	100%	2,8	443
NOVEMBER	98,36	1,64	-	100%	8,1	244
AVERAGE	77,88	22,12	-	100%	9,7	2766

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Bitdefender

Total Security

The workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,526 real malware samples, which translated into a maximum score of 100% of in-the-wild threats neutralized.

- Over 97% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Almost 3% of samples were blocked only after being executed.
- Bitdefender took an average of 1.7 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Bitdefender Total Security did not allow the operating system or data on the disk to be exposed to a potential leak as a result of malware execution.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	97,23	2,77	-	100%	1,8	759
MARCH	96,38	3,62	-	100%	3,1	607
MAY	94,22	5,78	-	100%	2,9	473
JULY			NOT TESTED			
SEPTEMBER	98,65	1,35	-	100%	0,5	443
NOVEMBER	100	-	-	100%	0,0	244
AVERAGE	97,30	3,38			1,7	2526

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

COMODO

Internet Security

The workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,522/2,523 real malware samples, which translated into a result of 99.92% of in-the-wild threats neutralized.

- Over 26% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Over 73% of samples were blocked only after being executed.
- Comodo took an average of 37.1 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that Comodo Internet Security only potentially led to a leak in one case as a result of malicious code execution. The incident was recorded and reported to the manufacturer; it was later determined that the malware sample had been mistakenly marked manually by an operator on Comodo's side. In all other cases, threats were effectively detected and neutralized without any negative impact on the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	34,26	60,53	-	100%	165,0	759
MARCH	28,17	54,68	-	100%	5,1	607
MAY	24,74	71,67	-	100%	5,4	473
JULY	24,58	64	0,42 (1)	99,58%	5,4	240
SEPTEMBER	20,77	73,14	-	100%	4,8	443
NOVEMBER			NOT TESTED			
AVERAGE	26,50	64,825	-	99,92%	37,1	2522

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Smart Security Premium

Workstation protection software participated in 3/6 editions of the test. Throughout the year, it blocked a total of 927 real malware samples, which translated into a maximum score of 100% of in-the-wild threats neutralized.

- Over 94% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 6% of samples were blocked only after being executed.
- Eset took an average of 0.13 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Eset Smart Security Premium did not allow the operating system or data on the disk to be exposed to a potential leak as a result of running malware.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH			NOT TESTED			
MAY			NOT TESTED			
JULY	91,25	8,75	-	100%	0,26	240
SEPTEMBER	95,71	4,29	-	100%	0,14	443
NOVEMBER	95,71	4,29	-	100%	0,00	244
AVERAGE	94,22	5,78	-	100%	0,13	927

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

EMSISOFT

Enterprise Security + EDR

Workstation protection software participated in all editions of the test. Throughout the year, it blocked a total of 2,766 real malware samples, which translated into a maximum score of 100% of in-the-wild threats neutralized.

- Nearly 57% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Over 43% of samples were blocked only after being executed.
- Emsisoft took an average of 31.2 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we can confirm that Emsisoft Enterprise Security with the EDR module did not allow a single instance of the operating system or data on disk to be exposed to potential leakage as a result of malware execution.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	27,27	72,73	-	100%	180	759
MARCH	28,01	72,99	-	100%	0,11	607
MAY	44,61	55,39	-	100%	0,04	473
JULY	68,75	31,25	-	100%	4,2	240
SEPTEMBER	87,36	12,64	-	100%	1,3	443
NOVEMBER	85,25	14,75	-	100%	1,76	244
AVERAGE	56,88	43,29	-	100%	31,2	2766

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

F-Secure

Total

Workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,525/2,526 real malware samples, which translated into a score of 99.92% of in-the-wild threats neutralized.

- Nearly 67% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Over 23% of samples were blocked only after being executed.
- F-Secure took an average of 39 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that F-Secure Total only potentially led to a leak in one case as a result of malicious code execution. In other cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	73,12	26,88	-	100%	1,05	759
MARCH	66,72	33,28	-	100%	8,0	607
MAY	83,72	15,86	0,42 (1)	99,58%	26,0	473
JULY			NOT TESTED			
SEPTEMBER	74,04	25,96	-	100%	54,0	443
NOVEMBER	13,52	86,48	-	100%	106,0	244
AVERAGE	66,84	37,69	-	99,92%	39,0	2526

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Total Protection

Workstation protection software participated in 4/6 editions of the test. Throughout the year, it blocked a total of 1,400 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Over 94% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Almost 6% of samples were blocked only after execution.
- G Data needed an average of 3.6 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that G Data Total Protection did not allow the operating system or data on the disk to be exposed to a potential leak as a result of malware execution even once.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH			NOT TESTED			
MAY	83,51	16,49	-	100%	8,5	473
JULY	95	5	-	100%	5,8	240
SEPTEMBER	98,65	1,35	-	100%	0,01	443
NOVEMBER	99,59	0,41	-	100%	0,11	244
AVERAGE	94,19	5,81	-	100%	3,6	1400

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

K7 SECURITY

Total Security

Workstation protection software participated in 3/6 editions of the test. Throughout the year, it blocked a total of 1,809 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Over 63% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 37% of samples were blocked only after being executed.
- K7 took an average of 6.1 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that K7 Total Security did not allow the operating system or data on the disk to be exposed to potential leakage as a result of malware execution even once.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	59,03	40,97	-	100%	11,8	759
MARCH	44,65	55,35	-	100%	5,1	607
MAY			NOT TESTED			
JULY			NOT TESTED			
SEPTEMBER	85,78	14,22	-	100%	1,4	443
NOVEMBER			NOT TESTED			
AVERAGE	63,15	36,85	-	100%	6,1	1809

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

Malwarebytes | Premium

Workstation protection software participated in all editions of the test. Throughout the year, it blocked a total of 2,766 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Nearly 83% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Over 17% of samples were blocked only after being executed.
- Malwarebytes took an average of 41.9 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Malwarebytes Premium did not once expose the operating system or data on the disk to potential leakage as a result of malware execution.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	62,98	38,02	-	100%	83	759
MARCH	56,01	43,99	-	100%	110	607
MAY	88,16	11,84	-	100%	27	473
JULY	97,57	2,43	-	100%	20,9	240
SEPTEMBER	92,29	2,71	-	100%	8,4	443
NOVEMBER	99,59	0,41	-	100%	2,18	244
AVERAGE	82,77	16,57	-	100%	41,9	2766

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

McAfee™ Total Protection

AV-LAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2026
ADVANCED IN-THE-WILD MALWARE TEST

Workstation protection software participated in 3/6 editions of the test. Throughout the year, it blocked a total of 1,522/1,523 real malware samples, which translated into a score of 99.93% of in-the-wild threats neutralized.

- Over 98% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 2% of samples were blocked only after being executed.
- McAfee took an average of 5.9 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that McAfee Total Protection only potentially led to a leak in one case as a result of malicious code execution. In all other cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH	97,2	2,8	-	100%	7,8	607
MAY	98,8	1	0,2 (1)	99,79%	7,8	473
JULY			NOT TESTED			
SEPTEMBER	99,1	0,9	-	100%	2,1	443
NOVEMBER			NOT TESTED			
AVERAGE	98,37	1,57	-	99,93%	5,9	1523

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Microsoft Defender

Workstation protection software participated in 4/6 editions of the test. Throughout the year, it blocked a total of 1,565/1,564 real malware samples, which translated into a score of 99.9% of in-the-wild threats neutralized.

- Over 31% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 69% of samples were blocked only after being executed.
- Microsoft needed an average of 38.4 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that Microsoft Defender only potentially led to a leak in one case as a result of malicious code execution. In other cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH	6,92	93,08	-	100%	49,10	607
MAY	9,94	90,06	-	100%	49,00	473
JULY	9,17	90,42	0,42 (1)	99,58%	54,20	240
SEPTEMBER			NOT TESTED			
NOVEMBER	97,95	2,05	-	100%	1,34	244
AVERAGE	31	68,9	-	99,90%	38,41	1564

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

mks_vir

Endpoint Security

Workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2006/2007 real-world malware samples, which translated into a score of 99.96% of in-the-wild threats neutralized.

- Over 80% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 20% of samples were blocked only after being executed.
- mks_vir needed an average of 7.7 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that mks_vir Endpoint Security only potentially led to a leak in one case as a result of malicious code execution. In other cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH	81,55	14,45	-	100%	2,9	607
MAY	78,22	21,56	0,21 (1)	99,79%	18	473
JULY	81,86	18,33	-	100%	3,9	240
SEPTEMBER	60,72	39,28	-	100%	4,4	443
NOVEMBER	97,95	2,05	-	100%	9,3	244
AVERAGE	80	19,1	-	99,96%	7,7	2007

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

norton™ Antivirus Plus

Workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,766 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Nearly 82% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Over 18% of samples were blocked only after being executed.
- Norton took an average of 1.24 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Norton Antivirus Plus did not allow the operating system or data on the disk to be exposed to a potential leak as a result of running malware.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH	52,39	47,61	-	100%	1,4	607
MAY	70,32	29,68	-	100%	2,2	473
JULY	93,75	6,25	-	100%	0,21	240
SEPTEMBER	96,61	3,39	-	100%	0,72	443
NOVEMBER	98,36	1,64	-	100%	1,66	244
AVERAGE	82	17,7	-	100%	1,24	2007

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Quick Heal
Security Simplified

Total Security

Workstation protection software participated in 3/6 editions of the test. Throughout the year, it blocked a total of 1,290 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Over 77% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 23% of samples were blocked only after being executed.
- Quick Heal took an average of 26.1 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Quick Heal Total Security did not allow the operating system or data on the disk to be exposed to potential leakage as a result of malware execution even once.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY			NOT TESTED			
MARCH	71,99	28,01	-	100%	36	607
MAY			NOT TESTED			
JULY	72,08	27,92	-	100%	28	240
SEPTEMBER	88,49	11,51	-	100%	14,3	443
NOVEMBER			NOT TESTED			
AVERAGE	77,52	22,48	-	100%	26,1	1290

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

ThreatDown
Powered by Malwarebytes

Endpoint Protection + EDR

Workstation protection software participated in all editions of the test. Throughout the year, it blocked a total of 2,766 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Over 84% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 16% of samples were blocked only after being executed.
- ThreatDown took an average of 38.4 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that ThreatDown Endpoint Protection with the EDR module did not allow the operating system or data on the disk to be exposed to a potential leak as a result of malware execution.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	64,56	35,44	-	100%	79	759
MARCH	58,65	41,35	-	100%	100	607
MAY	88,16	11,84	-	100%	28	473
JULY	97,92	2,18	-	100%	9,4	240
SEPTEMBER	97,74	2,26	-	100%	6,1	443
NOVEMBER	98,77	1,23	-	100%	8,01	244
AVERAGE	84,30	15,72	-	100%	38,4	2766

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Endpoint Protection

The workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,149/2,159 real malware samples, which translated into a score of 99.46% of in-the-wild threats neutralized.

- Over 89% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 11% of samples were blocked only after being executed.
- WatchGuard took an average of 25.6 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that WatchGuard Endpoint Protection potentially led to a leak in 10 cases as a result of malicious code execution. In the remaining cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	87,37	12,65	-	100%	0,01	759
MARCH			NOT TESTED			
MAY	82,88	16,28	0,85 (4)	99,15%	48	473
JULY	90,42	9,17	0,42 (1)	99,58%	29,0	240
SEPTEMBER	93	6,32	0,68 (3)	99,38%	18,2	443
NOVEMBER	94,26	4,92	0,82 (2)	99,18%	32,6	244
AVERAGE	89,59	9,87	-	99%	25,6	2159

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

WEBROOT by opentext™

Antivirus

Workstation protection software participated in all editions of the test. Throughout the year, it blocked a total of 2,766 real malware samples, which translated into a 100% neutralization rate for in-the-wild threats.

- Over 53% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 47% of samples were blocked only after being executed.
- Webroot took an average of 113 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we confirm that Webroot Antivirus did not allow the operating system or data on the disk to be exposed to a potential leak as a result of running malware.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	42,42	57,58	-	100%	112	759
MARCH	50,74	49,26	-	100%	126	607
MAY	41,52	58,48	-	100%	140	473
JULY	42,5	57,5	-	100%	137	240
SEPTEMBER	57,11	42,89	-	100%	135	443
NOVEMBER	85,25	14,75	-	100%	33	244
AVERAGE	53,26	46,74	-	100%	113,8	2766

WEB-LAYER PROTECTION (PRE-LAUNCH)**:** the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH)**:** the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL)**:** the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT)**:** average time based on all test editions

xcitium
The Power of Zero. Unleashed.

ZeroThreat Advanced + EDR

Workstation protection software participated in 5/6 editions of the test. Throughout the year, it blocked a total of 2,522/2,523 real malware samples, which translated into a score of 99.92% of in-the-wild threats neutralized.

- Over 20% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 80% of samples were blocked only after being executed.
- Xcitium took an average of 40.8 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that Xcitium ZeroThreat Advanced with the EDR module only potentially led to a leak in one case as a result of malicious code execution. The incident was recorded and reported to the manufacturer; it was later determined that the malware sample had been mistakenly marked manually by an operator on the Xcitium systems side. In all other cases, threats were effectively detected and neutralized without any negative impact on the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	5,8	94,2	-	100%	139	759
MARCH	41,68	58,32	-	100%	10,1	607
MAY	14,16	85,84	-	100%	20	473
JULY	31,67	67,92	0,42 (1)	99,58%	12	240
SEPTEMBER	10,16	89,84	-	100%	22,9	443
NOVEMBER			NOT TESTED			
AVERAGE	20,69	79,22		99,92%	40,8	2522

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

ZONEALARM By Check Point

Extreme Security

AV-LAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2026
ADVANCED IN-THE-WILD MALWARE TEST

Workstation protection software participated in 3/6 editions of the test. Throughout the year, it blocked a total of 1,834/1,839 real malware samples, which translated into a score of 99.72% of in-the-wild threats neutralized.

- Over 57% of threats were blocked at the browser stage or immediately after being saved to disk, without the malicious code being executed.
- Nearly 43% of samples were blocked only after being executed.
- ZoneAlarm took an average of 43 seconds to automatically and flawlessly repair security incidents.

Based on telemetry data, we conclude that ZoneAlarm Extreme Security potentially led to a leak in 5 cases as a result of malicious code execution. In the remaining cases, threats were effectively detected and neutralized without negatively impacting the operating system or user data.

	WEB-LAYER (%)	RUNTIME DEFENSE (%)	COMPROMISED (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	66,53	33,33	0,13 (1)	99,87%	31	759
MARCH	55,02	44,48	0,49 (3)	99,51%	47	607
MAY	50,11	49,68	0,21 (1)	99,79%	51	473
JULY			NOT TESTED			
SEPTEMBER			NOT TESTED			
NOVEMBER			NOT TESTED			
AVERAGE	57,22	42,50		99,72%	43,00	1839

WEB-LAYER PROTECTION (PRE-LAUNCH): the level concerns detecting malware samples before they are launched in the system.

RUNTIME DEFENSE (POST-LAUNCH): the level refers to the analysis of when a virus broke in into the system, was launched, and detected by the tested solutions.

SYSTEM COMPROMISED (FAIL): the malware was not blocked, and it infected the system.

REMEDIATION TIME (RT): average time based on all test editions

Why is it worth **taking part in the test?**

By participating in the tests, developers have a chance to learn about potential risks that may have been overlooked, or not taken into account.

Error Elimination
By engaging in cooperation, you will receive information about errors already at the investigation stage. This will help you take the right steps faster to fix potential bugs in software.

Acquiring Customers
The research results we publish reach potential customers who are looking for solutions to ensure their safety.

Product Certification
You can receive internationally recognized certificates that prove effective protection and reliable neutralization of threats throughout the year.

What information **will you get from the test?**

Example use of telemetry data from a test:

- **Was the threat stopped before it infected the system?**
- **Have the tested solution neutralized a threat in the system?**
- **How long did it take from the entry of an unknown file into the system to the recovery from a potential cyberattack?**
- **Which developer's technology does contribute to identifying and blocking a threat?**
- **Clear rules for developers and communities**

In 2025, as many as **10 developers improved their products** thanks to the tests we conducted!

What characterizes **our tests?**

To obtain malware, we use low and high interactive honeypots.

Test automation is provided by modern technologies and open source tools.

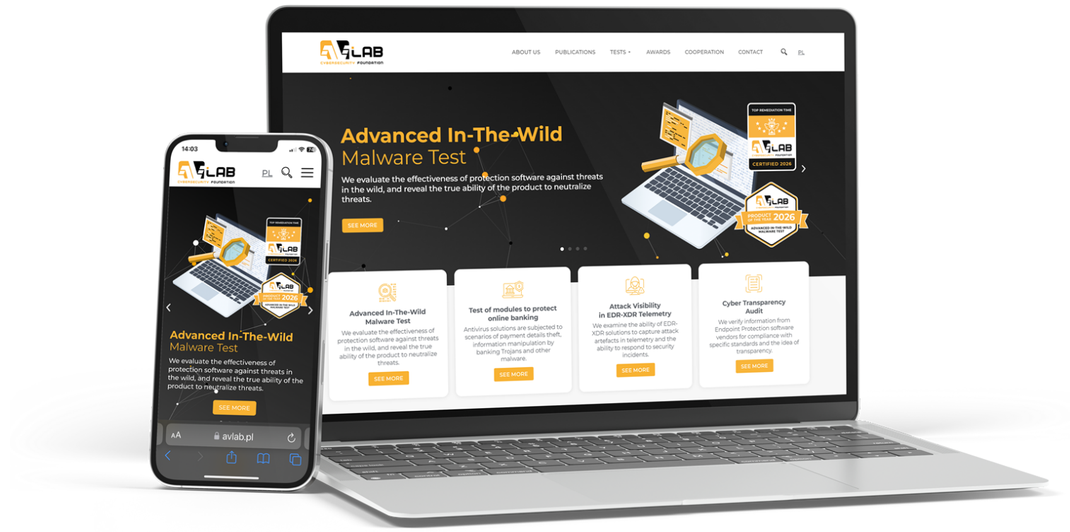
We use real methods to infect systems with malware instead of simulations.

We always provide developers with feedback from the tests carried out.

We draw attention to the weak points of protection software, and contribute to its improvement.

We work with leading cybersecurity companies to stay up to date with issues and threats in the digital world.

For more information, please visit our website: https://avlab.pl/en/advanced-in-the-wild-malware-test/



To learn more about the collaboration, please visit the webpage, where you can also read the results of recent editions.

CHECK OUR WEBSITE

We also conduct tests of other types:

Attack Visibility in EDR-XDR Telemetry

We examine the ability of EDR-XDR solutions to capture attack artefacts in telemetry and the ability to respond to security incidents.

Test of modules to protect online banking

Antivirus solutions are subjected to scenarios of payment details theft, information manipulation by banking Trojans and other malware.

Cyber Transparency Audit

We verify information from Endpoint Protection software vendors for compliance with specific standards and the idea of transparency.

CYBERSECURITY FOUNDATION

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet.

We are part of the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing. Also, we are a member of MVI (Microsoft Virus Initiative) in this matter as well.

We build awareness of users in the field of digital protection.
We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity.
Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation,
please refer to our full offer and contact us: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER