AVLAB
CYBERSECURITY FOUNDATION

Product of the Year 2025*

Recommended solutions for securing Windows 10/11 environment

AVLAB
CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB
CYBERSECURITY FOUNDATION
CERTIFIED 2025

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl

* Based on Advanced In-The-Wild Malware Test in 2024

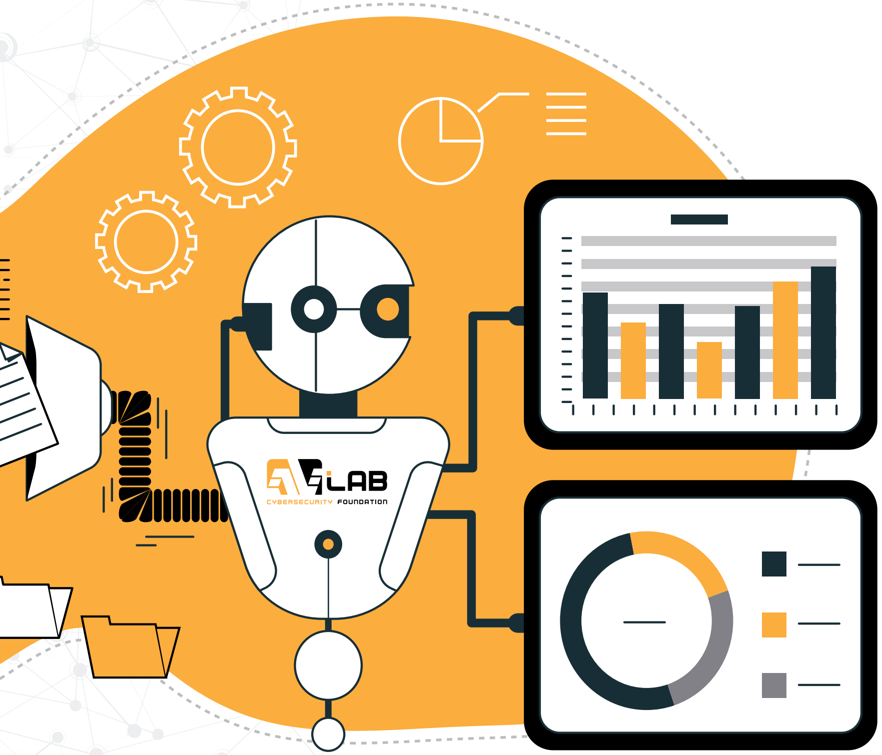
JANUARY 2025

Table of contents

Summary of Advanced In-The-Wild Malware Test in 2024

The purpose of this summary is to recognize the developers whose software participated in the research initiated by the AVLab Cybersecurity Foundation in 2024. The awarding of a special **"Product of the Year 2025"** award is an excellent opportunity to encourage individuals in IT managerial positions, heads of technology and security, who need to implement appropriate standards and procedures to ensure digital security with the best solutions.

In preparing the year-long test summary, we want to reward developers in two categories. The first category is the "Product of the Year 2025" award, which recognizes products that offer robust protection of the Windows operating system from a comprehensive perspective. This award emphasizes the behavior of the user who browses the Internet, downloads, and runs unknown, potentially malicious files.



The second award is the **"TOP Remediation Time 2025"** certificate, which is awarded for rapid remediation of malware once it has entered the system and is running. The TOP Remediation Time award recognizes an effective and timely response to malware that encompasses the entire life cycle of the malware - from the moment the sample enters the system to the removal of malicious activity, such as restarting the operating system or restoring data through the rollback feature.

The Advanced In-The-Wild Malware Test series is one of the most rigorous and meticulous tests available, revealing the protection product's capabilities against real-world threats that infiltrate computers through spam, instant messaging, or Web sites.

Our testing procedures involve evaluating solutions either on default settings or with additional security features enabled. If we determine that additional features should be activated or are required by the software developer, we always include a note in the report after each test edition.

Award criteria

The following criteria will be used to determine the winners

To be considered for the Product of the Year 2025 certificate, the tested solution had to meet specific criteria:

1. First, the solution had to participate in at least three editions of the Advanced In-The-Wild Malware Test. These tests are performed six times per year.
2. Secondly, obtain 3x EXCELLENT certification, demonstrating a minimum of 99% protection effectiveness.

Additional TOP Remediation Time 2025 certification:

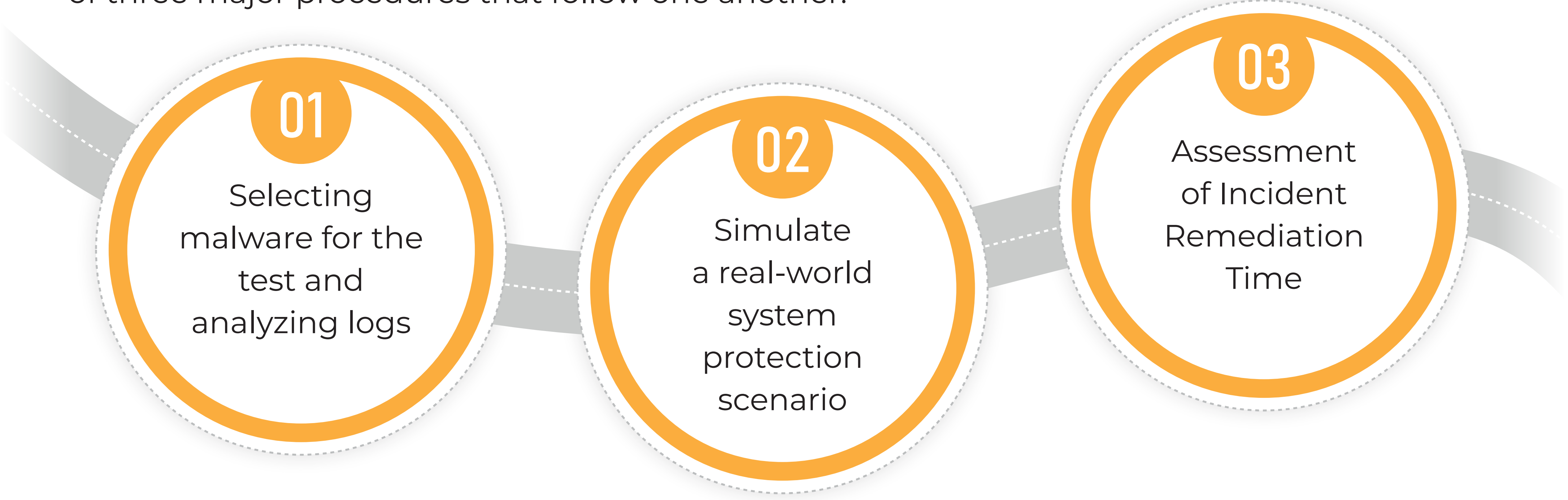
The software must neutralize all threats in at least three editions of the test and obtain a score of 100%. If the solution has been tested more than three times, we will consider the three results with the lowest average Remediation Time score.

What is the testing process? Information in a nutshell

The Advanced In-The-Wild Malware Test is a long-term analysis with the primary goal of verifying the effectiveness of tested solutions against malware in real time. In this test, we evaluate business versions of security products, which are often equipped with advanced EDR-XDR modules used to automatically hunt for threats along with remediation functionality for attacks. Additionally, we evaluate software versions tailored for individual users. In summary, we replicate a person's Internet browsing behavior after installing security software on Windows. This is the most common scenario in which individuals can fall victim to social engineering and inadvertently download malware to the system.

Real samples of in-the-wild malware from real URLs are selected for the test, so the test is most beneficial for all recipients and developers that participate in the study. At the conclusion of each edition, a comprehensive technical report is published detailing the threat detection and blocking methods used. In addition, using Windows systems in graphical mode, the test evaluates the real-world protection provided by the product, taking into account the remediation of each incident.

The results of the Advanced In-The-Wild Malware Test series consist of three major procedures that follow one another:



01 Selecting malware for the test and analyzing logs

02 Simulate a real-world system protection scenario

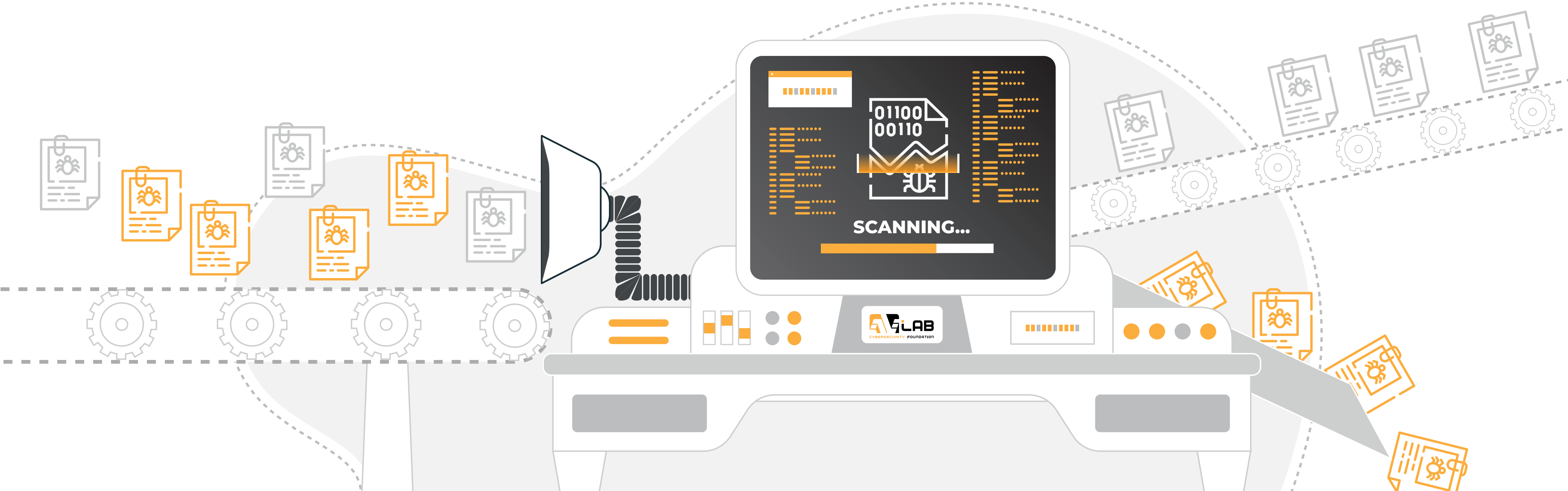
03 Assessment of Incident Remediation Time

1. Selecting malware for testing and analyzing logs

We collect malware in the form of real URLs from the Internet on an ongoing basis. Our approach involves leveraging a diverse array of samples from various sources, including public feeds, honeypot networks, and Telegram groups. The test encompasses the most current and diverse set of threats.

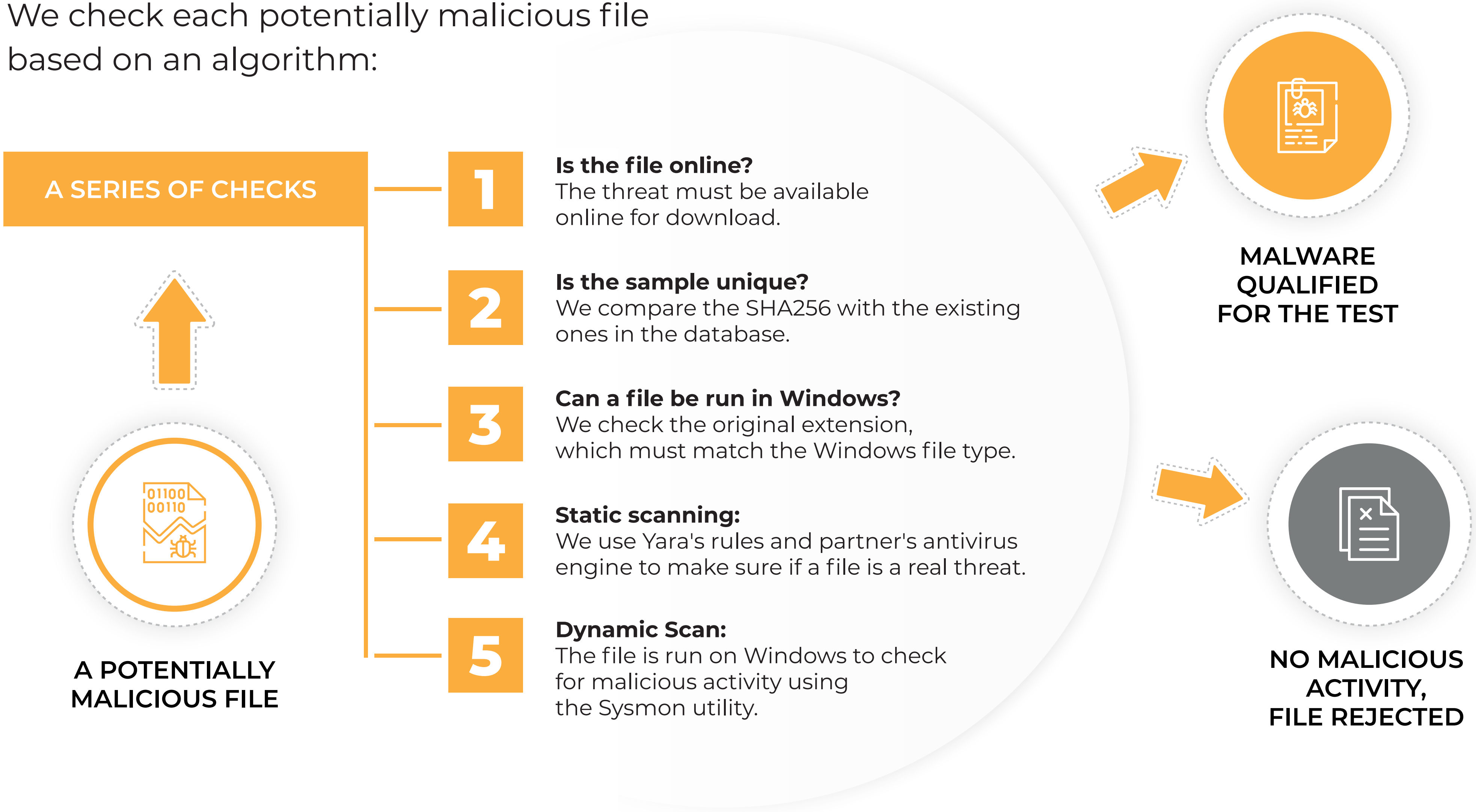
Each sample undergoes a rigorous series of checks before being sent for testing. One such check involves comparing the SHA256 sum with those already stored in the database. This guarantees that our tests do not involve the use of the same malware in multiple instances.

We meticulously analyze samples of potential malware using Windows verification based on hundreds of rules. These rules represent the most common techniques used by malware authors (known as LOLBin). We closely monitor system processes, network connections, the Windows registry, and other changes made to the operating system to determine the factors that led to the sample being classified as malicious during our analysis.



Algorithm for dealing with malware

We check each potentially malicious file based on an algorithm:



A SERIES OF CHECKS

1 **Is the file online?** The threat must be available online for download.

2 **Is the sample unique?** We compare the SHA256 with the existing ones in the database.

3 **Can a file be run in Windows?** We check the original extension, which must match the Windows file type.

4 **Static scanning:** We use Yara's rules and partner's antivirus engine to make sure if a file is a real threat.

5 **Dynamic Scan:** The file is run on Windows to check for malicious activity using the Sysmon utility.

A POTENTIALLY MALICIOUS FILE

MALWARE QUALIFIED FOR THE TEST

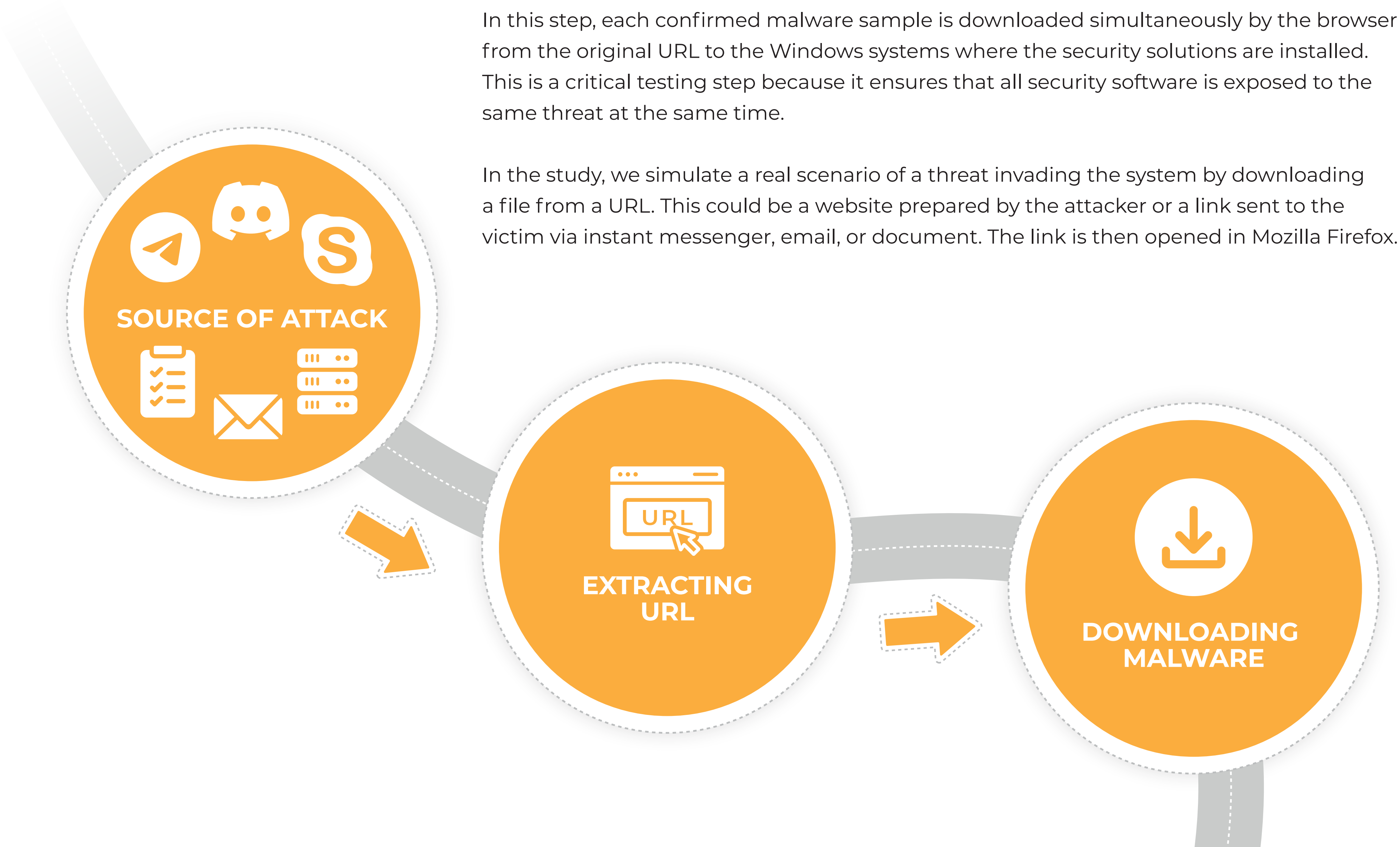
NO MALICIOUS ACTIVITY, FILE REJECTED

✱ Many of the threats evaluated in this test are distributed over the HTTPS protocol, which is often considered to be secure. Those who create malicious sites can easily and quickly obtain an SSL certificate to increase domain trust, and they do so at no cost. Some of these files are hosted on legitimate web servers. However, the actors leverage the domain's reputation to bypass the underlying security mechanisms.

2. Simulate a real system protection scenario

In this step, each confirmed malware sample is downloaded simultaneously by the browser from the original URL to the Windows systems where the security solutions are installed. This is a critical testing step because it ensures that all security software is exposed to the same threat at the same time.

In the study, we simulate a real scenario of a threat invading the system by downloading a file from a URL. This could be a website prepared by the attacker or a link sent to the victim via instant messenger, email, or document. The link is then opened in Mozilla Firefox.



The result on the malware sample can be classified into one of the following levels:

PRE-LAUNCH

The classification concerns detecting malware samples before they are launched in the system.

If the link to the file is quickly identified and blocked in the browser, or the file is deleted shortly after being saved to disk by the product under test, then we assign a so-called PRE-LANUCH score for the sample. In this case, the threat in question is stopped at an early stage, even before it is launched.

POST-LAUNCH

The analysis level, i.e. a virus has been run and blocked by a tested product.

If malware is downloaded and allowed to run but successfully stopped, we assign a POST-LANUCH level, assessing the product's real effectiveness against known threats and against 0-day threats.

FAIL

The failure, i.e. a virus hasn't been blocked and it has infected a system.

The Pre-Launch level indicates the detection and blocking of malware before it can execute its malicious payload, while the Post-Launch level refers to threats captured by vendor technology after the file has already been executed on the system. It is important to note that solutions with multiple layers of security, offering differentiated protection, tend to perform optimally at this level.

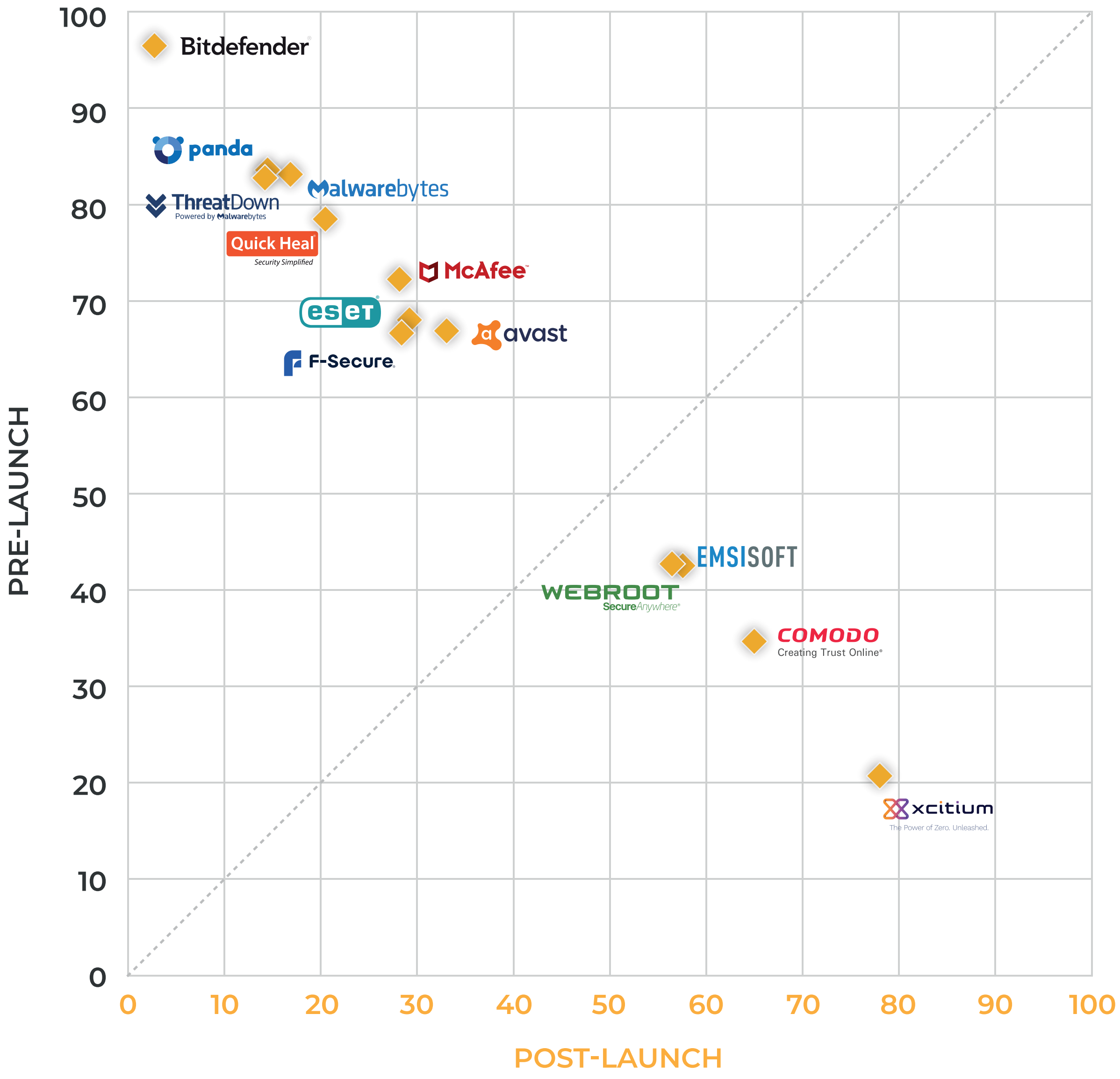
Security Solutions Protection Characteristics

A series of Advanced In-The-Wild Malware tests have demonstrated that solutions with multiple layers of protection are more effective against a broad range of Internet threats.

The vertical axis shows the level of threat detection and blocking before launch (PRE-Launch).

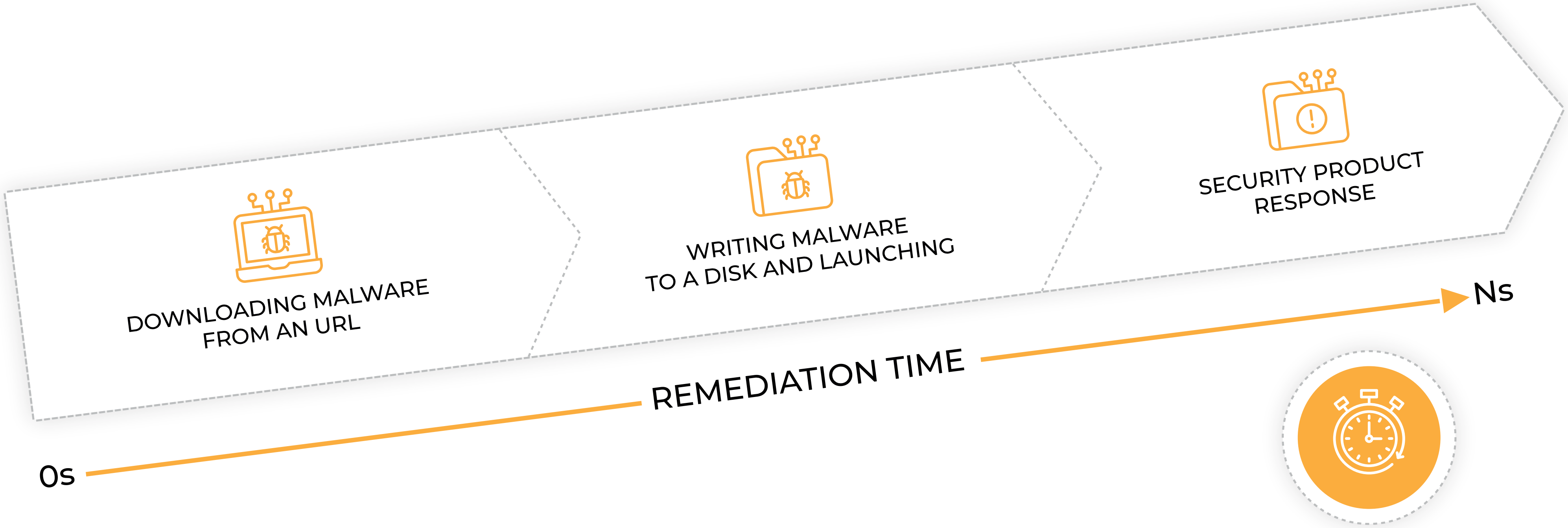
The horizontal axis indicates the neutralization and blocking of threats during the file access or post-launch phase (POST-Launch).

The solutions tested, which are above or below the diagonal line, are characterized by their respective styles of responding to threats at different stages of attack on a year-round basis across thousands of malware samples tested.



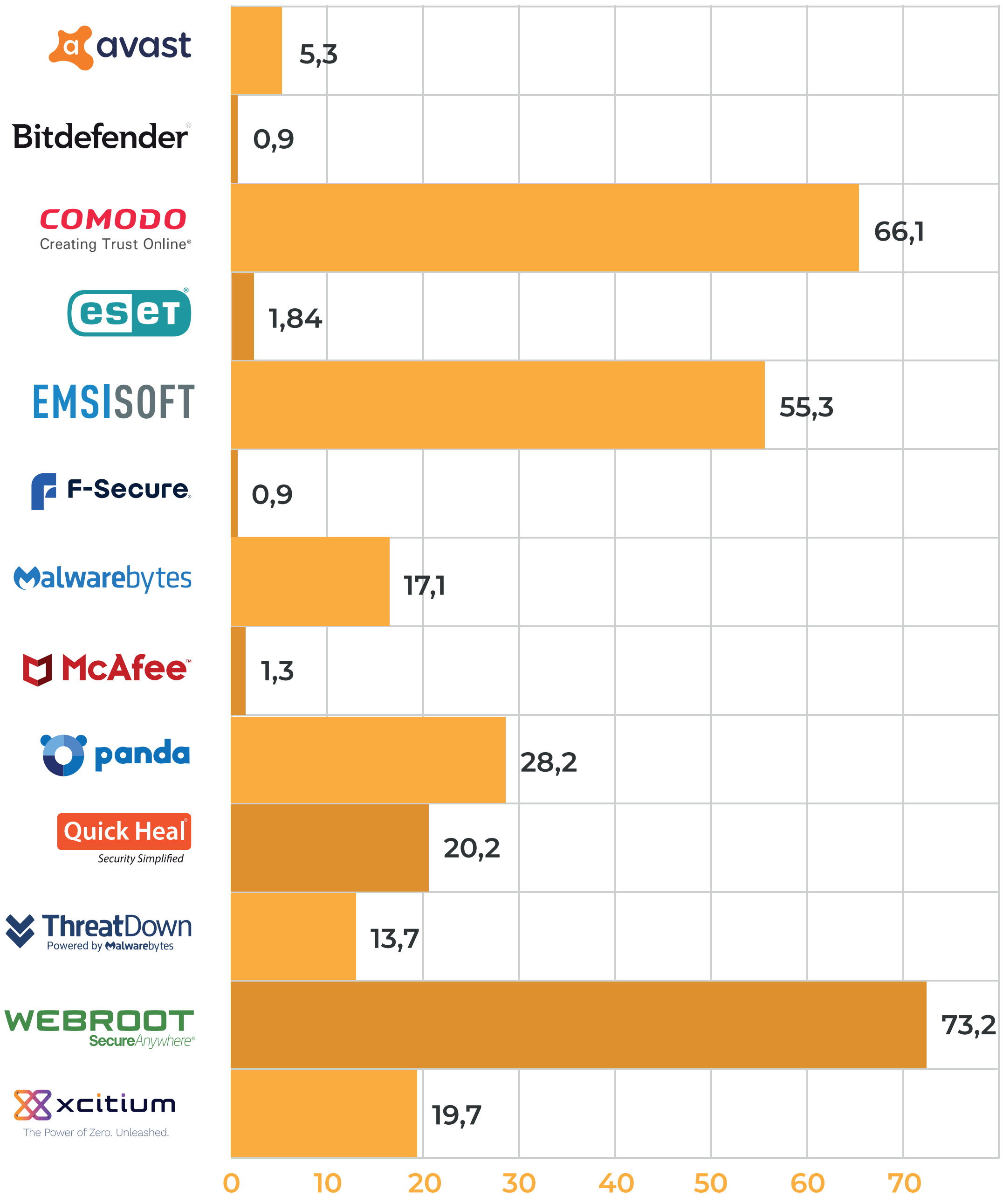
3. Incident remediation time assessment (Remediation Time)

Then, based on the logs obtained, in addition to detecting and blocking 0-day threats, we calculate the automatic remediation time of an incident for a given malware sample. We refer to this as the "Automatic Average Remediation Time." We configure the products under test so that the remediation of an attack with system repair is carried out automatically, without prompting the user to make a decision, as this is not the purpose of testing.


DOWNLOADING MALWARE FROM AN URL
WRITING MALWARE TO A DISK AND LAUNCHING
SECURITY PRODUCT RESPONSE
0s
REMEDIATION TIME
Ns

To estimate the average remediation time, it is assumed that the incident begins with a file download from the URL and continues until the dynamic analysis is completed, which takes 7 to 9 minutes. After this time, if no activity is detected by the security product, the analysis is completed with a negative result (Fail). Finally, for each malware sample, we measure the time it takes from the start to detect Indicators of Compromise (IoC) and to automatically remediate the incident.

Average Remediation Time in Tests Results



The Remediation Time indicator is an additional feature that describes a product. It indicates the time it takes for a sample to be detected from entry into the system (downloading malware from a URL), launch, to detection with remediation of the security incident. This time is measured for a sample that was stopped at the PRE-Launch level (still in the browser or just after saving to disk) as well as at the POST-Launch level. At the POST-Launch level, the malware is launched and the security solution responds (blocking access to the file, neutralizing, rolling back harmful changes).

We are the first lab to measure Remediation Time for each solution under test to more accurately indicate the differences between security software in the clash against Internet-based threats.

The time required for remediation, measured in seconds, is subject to variation depending on the product, configuration, vendor infrastructure, and other factors. In our testing procedures, we aim to configure the program to automate the re-sponse to threats.

Test statistics*

* Feedback is based on scanned files using the engine provided by our technology partner, mks_vir.

Basic information about malware

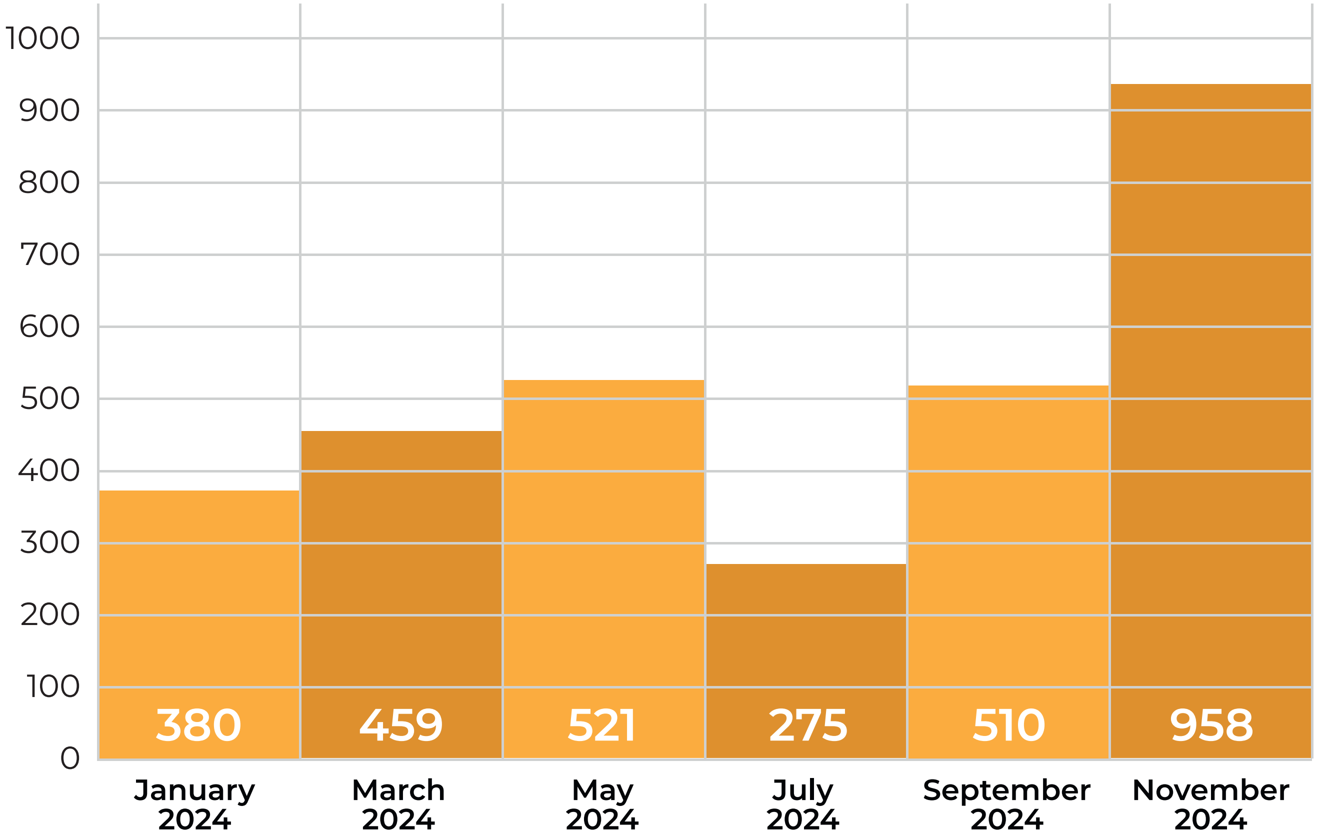
After reviewing the telemetry data from the tested solutions, we found that a total of 3,103 unique malware samples were used in 2024.

Malware in numbers

On average, 36% of all samples in each edition were threats that were not recognized on the day of analysis, corresponding to zero reputation (0-day) files. Our analysis revealed that the most prevalent malware was primarily malicious updates and fake installers masquerading as legitimate software.

TOP12 THREATS CLASSIFICATION

HEUR.RoundKick.W: 3957,
Exploit.RTF-ObfsStrm.Gen: 234,
Trojan.CryptZ.Marte.1.Gen: 217,
Exploit.RTF-ObfsObjDat.Gen: 185,
Trojan.Generic.D4666EE8: 133,
Trojan.Mint.Zard.25: 105,
Trojan.Kryptik.260: 100,
Trojan.Generic.D417BBBF: 96,
Trojan.Munp.1: 91,
Win32.Neshta.A: 91,
Trojan.Jalapeno.421: 89,
Trojan.Metasploit.A: 85,



* Due to the pre-selection of potential malware samples, the number of samples used in the test may exceed the number of malware samples in the dataset.

More information

FROM TESTS IN 2024

6

EDITIONS OF THE ADVANCED IN-THE-WILD MALWARE TEST

3103

UNIQUE MALWARE IN TOTAL

36%

OF 0-DAY FILES IN EACH EDITION OF THE TEST (AVERAGE)

62%

PRE-LANUCH LEVEL OF MALWARE DETECTION (AVERAGE)

38%

POST-LANUCH LEVEL OF MALWARE BLOCKING (AVERAGE)

43s

AVERAGE REMEDIATION TIME TO RECOVER FROM INCIDENTS

Technology providers tested in 2024

avast

Bitdefender

CEGIS CYBER

COMODO
Creating Trust Online

EMSISOFT

eset

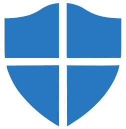
F-Secure

K7 SECURITY

kaspersky

Malwarebytes

McAfee



panda

Quick Heal
Security Simplified

ThreatDown
Powered by Malwarebytes

WEBROOT
SecureAnywhere

xcitium
The Power of Zero. Unleashed.

This is not a complete list, as some developers participate in tests anonymously to improve security technologies. Companies that are interested in testing their solutions, and would like to know what they can improve in their software, please contact us.

We invite you to view the results of the products certified in this study.

avast

Free Antivirus

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 67% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 32% of the malware samples were successfully blocked after launch.
- According to the top three scores, Avast software had an average response time of 5.3 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the AVAST Free Antivirus software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	71,05	28,95	-	100%	4,0	380
MARCH	74,07	25,93	-	100%	10,0	459
MAY	60,06	39,94	-	100%	8,2	521
JULY	65,82	34,18	-	100%	4,8	275
SEPTEMBER	55,69	44,31	-	100%	8,7	510
NOVEMBER	77,97	22,03	-	100%	7,2	958
AVERAGE	67,44	32,56	-	100%	5,3	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

Bitdefender® | Total Security

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

The workstation protection software was included in four editions of the test. During the year, it blocked 2211/2213 threats. This results in an almost maximum score for neutralized in-the-wild threats.

- More than 96% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- Nearly 4% of the malware samples were successfully blocked after launch.
- According to the top three scores, Bitdefender software had an average response time of 0.9 seconds to automatically and accurately address security incidents.

After reviewing the telemetry data, we can confirm that the BITDEFENDER Total Security software did not expose the operating system and data to potential leakage as a result of running malware on the test system. The two reported incidents do not meet the criteria for TOP Remediation Time certification.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	-	-	NOT TESTED		-	-
MARCH	91,58	8,16	0,22 (1 sample)	99,78%	1,48	459
MAY	97,98	2,02	-	100%	0,85	521
JULY	99,27	0,73	-	100%	0,01	275
SEPTEMBER	-	-	NOT TESTED		-	-
NOVEMBER	97,08	2,82	0,1 (1 sample)	99,90%	1,87	958
AVERAGE	96,48	3,43	-	100%	0,9	2213

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

COMODO
Creating Trust Online®

Internet Security

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 34% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 65% of the malware samples were successfully blocked after launch.
- According to the top three scores, Comodo software had an average response time of 66 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the COMODO Internet Security software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	34,97	60,53	-	100%	92,0	380
MARCH	45,32	54,68	-	100%	44,0	459
MAY	28,39	71,67	-	100%	138,0	521
JULY	36	64	-	100%	62,3	275
SEPTEMBER	26,86	73,14	-	100%	112,3	510
NOVEMBER	35,07	64,93	-	100%	167,0	958
AVERAGE	34,435	64,825	-	100%	66,1	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

Smart Security Premium

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

The workstation protection software was included in four editions of the test. During the year, it blocked 2210/2213 threats. This results in an almost maximum score for neutralized in-the-wild threats.

- Nearly 70% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- Nearly 30% of the malware samples were successfully blocked after launch.
- According to the top three scores, Eset software had an average response time of 1.8 seconds to automatically and accurately address security incidents.

After reviewing the telemetry data, we can confirm that the ESET Smart Security Premium software did not expose the operating system and data to potential leakage as a result of running malware on the test system. The three reported incidents do not meet the criteria for TOP Remediation Time certification.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	-	-	NOT TESTED		-	-
MARCH	75,38	24,4	0,22 (1 sample)	99,78%	1,43	459
MAY	54,88	44,93	0,19 (1 sample)	99,81%	1,93	521
JULY	73,82	26,18	-	100,00%	1,40	275
SEPTEMBER	-	-	NOT TESTED		-	-
NOVEMBER	75,68	24,22	0,1 (1 sample)	99,90%	2,20	958
AVERAGE	69,94	29,9325			1,84	2213

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

EMSISOFT

Enterprise Security + EDR

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- Nearly 43% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 58% of the malware samples were successfully blocked after launch.
- According to the top three scores, Emsisoft software had an average response time of 55 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the EMSISOFT Enterprise Security software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	52,89	47,11	-	100%	67,0	380
MARCH	51,85	54,68	-	100%	82,0	459
MAY	35,61	64,39	-	100%	114,0	521
JULY	45,45	54,55	-	100%	103,4	275
SEPTEMBER	51,18	48,82	-	100%	17,0	510
NOVEMBER	20,88	79,12	-	100%	184,0	958
AVERAGE	42,98	58,11	-	100%	55,3	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

F-Secure

Total

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

The workstation protection software was included in all editions of the test. During the year, it blocked 3101/3103 threats. This results in an almost maximum score for neutralized in-the-wild threats.

- Nearly 69% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 31% of the malware samples were successfully blocked after launch.
- According to the top three scores, F-Secure software had an average response time of 0.9 seconds to automatically and accurately address security incidents.

After reviewing the telemetry data, we can confirm that the F-SECURE Total software did not expose the operating system and data to potential leakage as a result of running malware on the test system.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	71,32	28,24	0,26 (1 sample)	99,74%	5,0	380
MARCH	87,7	12,2	-	100,00%	0,5	459
MAY	68,63	31,13	0,19 (1 sample)	99,81%	1,5	521
JULY	73,82	26,18	-	100,00%	0,8	275
SEPTEMBER	41,18	58,82	-	100,00%	1,7	510
NOVEMBER	70,46	29,54	-	100,00%	1,3	958
AVERAGE	68,85	31,02		99,93%	0,9	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

Malwarebytes Premium

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 82% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 17% of the malware samples were successfully blocked after launch.
- According to the top three scores, Malwarebytes software had an average response time of 17 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the MALWAREBYTES Premium software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	69,21	30,79	-	100%	41,0	380
MARCH	86,93	13,07	-	100%	20,0	459
MAY	78,32	21,38	-	100%	44,0	521
JULY	92,36	7,64	-	100%	15,3	275
SEPTEMBER	90,98	9,02	-	100%	16,0	510
NOVEMBER	76,62	23,38	-	100%	54,0	958
AVERAGE	82,40	17,55	-	100%	17,1	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

McAfee™ Total Protection

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

The workstation protection software was included in four editions of the test. During the year, it blocked 1635 threats. This result is maximum score for neutralized in-the-wild threats.

- More than 72% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 27% of the malware samples were successfully blocked after launch.
- According to the top three scores, McAfee software had an average response time of 1.3 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the MCAFEE Total Protection software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	2,63	97,37	-	100%	108,0	380
MARCH	91,07	8,93	-	100%	1,2	459
MAY	99,3	0,7	-	100%	0,6	521
JULY	98,91	1,09	-	100%	2,1	275
SEPTEMBER	-	-	NOT TESTED		-	510
NOVEMBER	-	-	NOT TESTED		-	958
AVERAGE	72,98	27,02	-	100,00%	1,3	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

panda

Dome Advanced

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

Workstation security software was included in all editions of the test. During the year, it blocked 3086/3103 threats. This result is particularly noteworthy when considering threat neutralization in the wild.

- Nearly 84% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 14% of the malware samples were successfully blocked after launch.
- According to the top three scores, Panda software had an average response time of 28.2 seconds to automatically and accurately address security incidents.

After reviewing the telemetry data, we can confirm that PANDA Dome Advanced software did not expose the operating system and data to significant leaks as a result of running malware on the test system. The solution does not meet the TOP remediation time certification criteria due to multiple reported incidents.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	85,53	13,95	0,53 (2 samples)	99,47%	18,00	380
MARCH	86,27	13,51	0,22 (1 sample)	99,78%	24,00	459
MAY	77,83	21,05	1,12 (7 samples)	98,88%	40,00	521
JULY	86,18	13,82	-	100%	27,60	275
SEPTEMBER	84,71	14,71	0,59 (3 samples)	99,41%	26,60	510
NOVEMBER	84,97	15,03	-	100%	33,00	958
AVERAGE	83,95	14,49		99,59%	28,20	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

ThreatDown
Powered by Malwarebytes

Endpoint Protection

AVLab CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLab CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 84% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 16% of the malware samples were successfully blocked after launch.
- According to the top three scores, ThreatDown Endpoint Protection software had an average response time of 13.7 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the THREATDOWN Endpoint Protection software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	64,97	30,53	-	100%	34,0	380
MARCH	88,02	11,92	-	100%	17,0	459
MAY	88,22	19,78	-	100%	36,0	521
JULY	93,45	6,55	-	100%	10,4	275
SEPTEMBER	91,37	8,63	-	100%	13,6	510
NOVEMBER	77,45	22,55	-	100%	48,0	958
AVERAGE	83,91	16,66	-	100%	13,7	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

Quick Heal®
Security Simplified

Total Security

PRODUCT OF THE YEAR 2025
AVLAB CYBERSECURITY FOUNDATION
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

The workstation protection software was included in four editions of the test. During the year, it blocked 1754 threats. This result is maximum score for neutralized in-the-wild threats.

- More than 79% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- More than 27% of the malware samples were successfully blocked after launch.
- According to the top three scores, Quick Heal software had an average response time of 20 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the QUICK HEAL Total Security software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	-	-	NOT TESTED		-	380
MARCH	-	-	NOT TESTED		-	459
MAY	80,52	19,48	-	100%	13,3	521
JULY	78,91	21,09	-	100%	18,3	275
SEPTEMBER	-	-	NOT TESTED		-	510
NOVEMBER	78,91	21,09	-	100%	29,0	958
AVERAGE	79,45	20,55	-	100,00%	20,2	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

WEBROOT®
by opentext™

Antivirus

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 43% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- Nearly 57% of the malware samples were successfully blocked after launch.
- According to the top three scores, Webroot software had an average response time of 73 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the WEBROOT Antivirus software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	51,11	47,63	0,26 (1 sample)	99,74%	28,0	380
MARCH	42,05	57,95	-	100%	69,0	459
MAY	41,99	58,01	-	100%	95,0	521
JULY	40,36	59,64	-	100%	75,6	275
SEPTEMBER	35,1	64,9	-	100%	74,9	510
NOVEMBER	48,64	51,36	-	100%	113,0	958
AVERAGE	43,21	56,58	-	99,96%	73,2	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

xcitium

The Power of Zero. Unleashed.

ZeroThreat Advanced + EDR

AVLAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2025
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AVLAB CYBERSECURITY FOUNDATION
CERTIFIED 2025

Workstation security software was included in all editions of the test. During the year, it blocked 3,103 threats. This gives a maximum score of 100% of all neutralized in-the-wild threats.

- More than 21% of threats were either blocked in the browser or prevented from executing after being saved to disk.
- Nearly 79% of the malware samples were successfully blocked after launch.
- According to the top three scores, Webroot software had an average response time of 19.7 seconds to automatically and accurately address security incidents.

According to the telemetry data obtained, we can confirm that the XCITIUM ZeroThreat Advanced software has not exposed the operating system or the data on the disk to potential leakage due to the launch of malware.

Test Environment: Windows 11 Pro

	PRE (%)	POST (%)	FAIL (%)	COMBINED PROTECTION	AVERAGE RT (s)	MALWARE USED
JANUARY	41,48	58,42	-	100%	54,0	380
MARCH	8,28	91,72	-	100%	12,0	459
MAY	18,18	81,82	-	100%	39,0	521
JULY	3,64	96,36	-	100%	27,2	275
SEPTEMBER	2,75	97,25	-	100%	19,8	510
NOVEMBER	52,61	47,39	-	100%	69,0	958
AVERAGE	21,16	78,83	-	100,00%	19,7	3103

PRE-LAUNCH: the level concerns detecting malware samples before they are launched in the system.

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.

FAIL: the malware was not blocked, and it infected the system.

RT [REMEDIATION TIME]: average time based on the top 3 results.

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**

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.

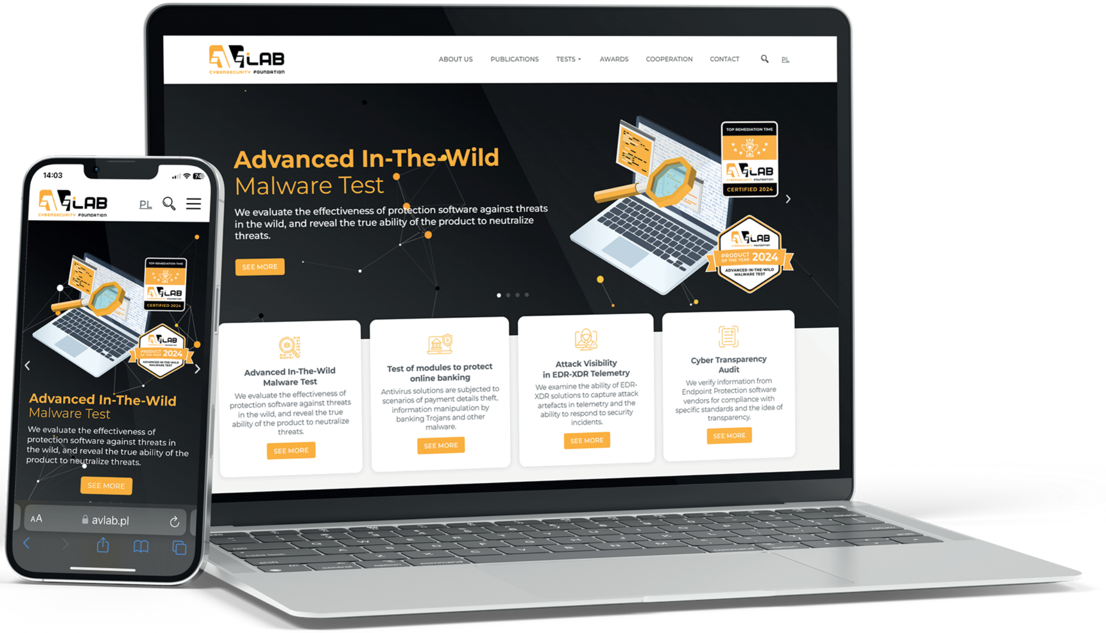
We draw attention to the weak points of protection software, and contribute to its improvement.

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

In 2024, as many as 10 developers improved their products thanks to the tests we conducted!

To learn more about the collaboration, please visit the Advanced In-The-Wild Malware Test page, where you can also track the results of recent editions.

CHECK OUR WEBSITE



AVLAB CYBERSECURITY FOUNDATION

ABOUT US · PUBLICATIONS · TESTS ▸ · AWARDS · COOPERATION · CONTACT · PL

Advanced In-The-Wild
Malware Test

We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.

SEE MORE

TOP REMEDIATION TIME · AVLAB CYBERSECURITY FOUNDATION · CERTIFIED 2024

AVLAB CYBERSECURITY FOUNDATION · PRODUCT OF THE YEAR 2024 · ADVANCED IN-THE-WILD MALWARE TEST

Advanced In-The-Wild Malware Test
We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.
SEE MORE

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.
SEE MORE

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.
SEE MORE

Cyber Transparency Audit
We verify information from Endpoint Protection software vendors for compliance with specific standards and the idea of transparency.
SEE MORE

14:03

AVLAB CYBERSECURITY FOUNDATION · PL

Advanced In-The-Wild
Malware Test

We evaluate the effectiveness of protection software against threats in the wild, and reveal the true ability of the product to neutralize threats.

SEE MORE

AA avlab.pl

We also conduct tests of other types:

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.

Attack Visibility in EDR-XDR Telemetry

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

Cyber Transparency Audit

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

For more information, please visit our website...

AVLAB

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.

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

www.avlab.pl