SE LABS ®

EDR PROTECTION MACOS

Security Evaluation Test Report

macOS Home Anti-Malware

ONLINE REPORT

SEPTEMBER 2026

SE Labs tested macOS with and without anti-malware products against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

We test like hackers, behaving like real attackers and probing targets with a variety of tools, techniques and vectors before attempting to gain access. Once we have access at a basic level we try to boost our power on the system before attempting to complete the mission, which might include stealing information, hiding our tracks and even damaging the target systems.

Contents

Document version 1.0 Written 25th August 2026

SE LABS

Management
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Technical Director Thomas Bean

Testing Team
Nikki Albesa
Daniel Botez
Solandra Brewster
Billy Coyne
Jarred Earlington
Gia Gorbold
Jake Hearn
Anila Johny
Cameron Love
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Enejda Torba

Marketing
Sara Claridge
Isobel Edwards

Publication
Rahat Hussain
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog https://selabs.uk/blog/
Post SE Labs Ltd,
55A High Street,
Wimbledon,
SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2022 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

CEO
Simon Edwards

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our website and follow us on LinkedIn.

Is Apple's macOS hack-proof?

Do you need anti-virus to stop targeted attacks on a Mac?

This test aims to assess the security built into macOS, the operating system that runs Apple's desktop and laptop personal computers. We also wanted to evaluate the usefulness and effectiveness of anti-virus (aka endpoint security) on macOS against targeted attacks.

If macOS' in-built security is sufficiently strong, it might not be technically necessary to use anti-virus. You might be able to rely on the security features built into the operating system.

If it's not sufficiently strong then the next question is, "are popular third-party anti-virus solutions good enough to add value." In other words, do you need anti-virus on a Mac to stop targeted attacks?

We created targeted attacks using common tools available to, and frequently used by attackers in the real world. The testing team then confirmed that these attacks were viable - that they worked against macOS systems with security settings disabled.

Once we had a library of functional attacks we set up two sets of targets. All targets were Mac computers with security settings enabled. We installed anti-virus software on these.

We chose five well-known anti-malware products that frequently appear in reviews and web searches. Most claim to offer protection against threats in real-time (not just as scans after an attack).

Targeted attacks are used to take control of a computer and achieve some aim, such as stealing or damaging data. It is not always necessary for an attacker to retain control (aka persistence) to achieve this goal. So the earlier the anti-virus detects the attack, the better.

How well did macOS protect against the threats? Did the anti-virus products help at all? Read on to find out how safe your Mac is.

Executive Summary

Without accurate test reports, most people can only rely on anti-malware companies' marketing claims. Apple does not make overt promises about preventing malware and similar threats but implies heavily that its platform is secure. The headline of its security page is, "Security. Built right in."

Despite that, our report shows that macOS requires a third-party anti-malware application to defend against targeted attacks. The protection built into the operating system is not sufficient to detect or prevent attacks from a skilled attacker.

The solutions that we chose to test were popular in reviews and internet search results. Most well-known brands performed very well in this test, protecting the system against all attacks. In most cases the attack was stopped at the very beginning.

Notably one solution did not detect or protect from any of the attacks as they occurred. It noticed a malicious file in a few of the attacks, but did not prevent us from gaining remote access, stealing information and damaging the system.

Products Tested	Protection Accuracy (%)
Bitdefender Antivirus for Mac	100%
ESET Home Security Essential	100%
Gen Digital Norton 360	100%
TotalAV Premium	100%
Canimaan Software ClamXAV	-125%
macOS	-125%

● Products highlighted in green were the most accurate, scoring 90 per cent or more for Total Accuracy. Those in orange scored less than 90 but 71 or more. Products shown in red scored less than 71 per cent.

Security Evaluation Test Award

The following product wins the SE Labs award:

Bitdefender Antivirus for Mac

ESET Home Security Essential

Gen Digital Norton 360

TotalAV Premium

1. Protection Details

1.1 Protection Details

These results break down how each product handled threats into some detail. You can see how many detected a threat and the levels of protection provided.

Products sometimes detect more threats than they protect against. This can happen when they recognise an element of the threat but aren't equipped to stop it. Products can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Product	Detected	Blocked	Neutralised	Compromised	Protected
Bitdefender Antivirus for Mac	11	11	0	0	11
ESET Home Security Essential	11	11	0	0	11
Gen Digital Norton 360	11	11	0	0	11
TotalAV Premium	11	11	0	0	11
Canimaan Software ClamXAV	5	0	0	11	0
macOS	0	0	0	11	0

- **This data shows in detail how each product handled the threats used.**

2. How We Tested

Threat Responses

Full Attack Chain: Testing Every Layer of Detection and Protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means that, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack Stages

The illustration (below) shows typical stages of an attack. In a test, each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

We measure how a product responds to the first stages of the attack with a detection and/or protection rating. Sometimes products allow threats to run yet still detect them. Other times they might allow the threat to run briefly before neutralising it. Ideally, they detect and block the threat before it has a chance to run. Products may delete threats or automatically contain them in a 'quarantine' or other safe holding mechanism for later analysis.

Should the initial attack phase succeed, we then measure post-exploitation stages, which are represented by steps two through to seven below. We broadly categorise these stages as:

Access (step 2); Action (step 3); Escalation (step 4); and Post-Escalation (steps 5-6).

In figure 1. you can see a typical attack running from start to end, through various 'hacking' activities. This can be classified as a fully successful breach.

In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

Attack Details

When testing services against targeted attacks it is important to ensure that the attacks used are relevant. Anyone can run an attack randomly against someone else. It is the security vendor's challenge to identify common attack types and to protect against them. As testers, we need to generate threats that in some way relate to the real world.

All of the attacks used in this test are valid ways to compromise a home computer. Without any security in place, all would succeed in attacking the target. Outcomes would include systems infected with ransomware, remote access to networks and data theft.

But we didn't just sit down and brainstorm how we would attack different people. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to those faced by targets all over the world.

In this test we could have taken well-known threats, known by every reputed anti-malware company, and run them on the target Mac computers. But there are three big problems with that approach.

The first is that there isn't much in the way of general malware for macOS, relatively speaking. It's a growing problem, but there is a vastly larger amount attacking Microsoft Windows PCs on a regular basis. The Mac malware situation is getting worse, but slowly. We think that targeted attacks are a much more serious problem.

The second problem with testing using well-known malware is that you can't tell if the anti-malware products are able to recognise new threats, or just rely on old knowledge of established threats.

Finally, using random malware samples from the internet does not give testers the control they need to penetrate the targets and potentially trigger different levels of defence. To do that, testers need to control the attacks fully.

To solve all of these problems we created targeted attacks against the users of our Mac computers. We used known tools but created previously unseen malware. If a product can detect our attacks and stop us, it's reasonable to assume it would do the same for you, should you face an attacker online. If it fails, you might treat its claims of providing protection with some scepticism.

In keeping with our usual approach, we didn't just create a single file that should be stopped. Instead we built a library of attacks that allowed us to take a basic level of control of the target systems and then we began to dig deeper, gaining greater power over the system.

We delivered these attacks via email, in so-called 'spear phishing' attacks. These are highly targeted emails designed to trick recipients into downloading and running malicious code on their systems. Once we establish control we follow a playbook of actions, which are commonly used by attackers.

In essence, we gathered system information; stole files; spied on the network; destroyed and encrypted data as a ransomware attackers would; and tried to hide our tracks.

To achieve some of these tasks we needed to escalate privileges, which we were able to do when there was no third-party real-time protection in play.

3. Response Details

In this test security products are exposed to attacks, which comprise multiple stages. The perfect product will detect and protect against all relevant elements of an attack. The term 'relevant' is important, because if early stages of an attack are countered fully there is no need for later stages to be addressed.

In each test case the product can score a maximum of four points for successfully detecting the attack and protecting the system from ill effects. If it fails to act optimally in any number of ways it is penalised, to a maximum extent of -9 (so -5 points in total). The level of penalisation is according to the following rules, which illustrate the compound penalties imposed when a product fails to prevent each of the stages of an attack.

Detection (-0.5)

If the product fails to detect the threat with any degree of useful information, it is penalised by 0.5 points.

Execution (-0.5)

Threats that are allowed to execute generate a penalty of 0.5 points.

Action (-1)

If the attack is permitted to perform one or more actions, remotely controlling the target, then a further penalty of 1 point is imposed.

Privilege Escalation (-2)

As the attack impact increases in seriousness, so do the penalties. If the attacker can escalate system privileges then an additional penalty of 2 points is added to the total.

Post-escalation Action (-1)

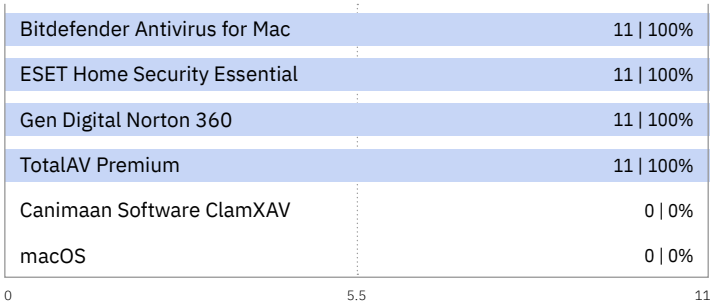
New, more powerful and insidious actions are possible with escalated privileges. If these are successful, the product loses one more point.

The Protection Rating is calculated by multiplying the resulting values by 4. The weighting system that we've used can be adjusted by readers of this report, according to their own attitude to risk and how much they value different levels of protection. By changing the penalisation levels and the overall protection weighting, it's possible to apply your own individual rating system.

The Total Protection Rating is calculated by multiplying the number of Protected cases by four (the default maximum score), then applying any penalties. Finally, the total is multiplied by four (the weighting value for Protection Ratings) to create the Total Protection Rating.

3.1 Detection Accuracy Ratings

To understand how we calculate these ratings, see **Response Details** on page 9.



● **Detection Ratings are weighted to show that how products detect threats can be subtler than just 'win' or 'lose'.**

Response Details

Target/Anti-Malware Solution	Number of Incidents	Protection	Detection	Delivery	Execution	Action	Privilege Escalation	Penalties
Bitdefender Antivirus for Mac	11	11	11	11	0	0	0	0
ESET Home Security Essential	11	11	11	11	0	0	0	0
Gen Digital Norton 360	11	11	11	11	0	0	0	0
TotalAV Premium	11	11	11	11	0	0	0	0
Canimaan Software ClamXAV	11	0	0	11	11	11	11	11
macOS	11	0	5	11	11	11	11	11

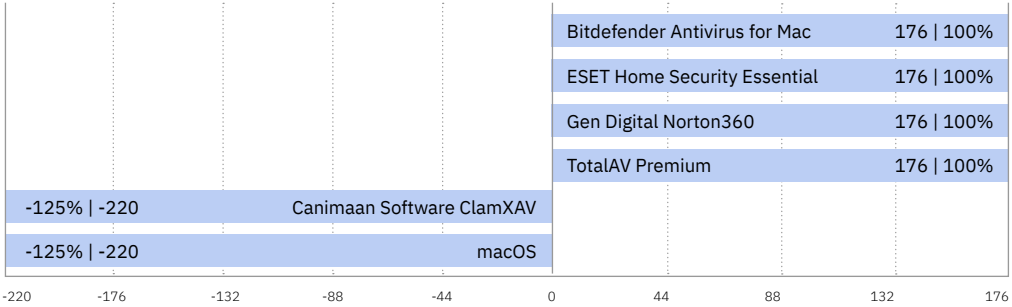
- This data shows how the product handled different stages of each attack. The columns labelled 'Delivery' through to 'Lateral Action' show how many times an attacker succeeded in achieving those goals. A 'zero' result is ideal.

Protection Accuracy Rating Details

Target/ Anti-Malware Solution	Number of Incidents	Protected	Penalties	Protection Score	Protection Rating
Bitdefender Antivirus for Mac	11	11	0	44	176
ESET Home Security Essential	11	11	0	44	176
Gen Digital Norton 360	11	11	0	44	176
TotalAV Premium	11	11	0	44	176
Canimaan Software ClamXAV	11	0	11	-55	-220
macOS	11	0	11	-55	-220

- Different levels of protection, and failure to protect, are used to calculate the Protection Rating.

3.2 Protection Accuracy Ratings



- Detection Ratings are weighted to show that how products detect threats can be subtler than just 'win' or 'lose'.

4. Conclusion

This report looks at how effectively macOS can protect against a range of targeted attacks. It also examines the abilities of five well-known Mac anti-malware products. Most claim to provide real-time protection against viruses and similar threats. One does not overtly claim instant protection, and the evidence from this test suggests that it has very limited capabilities in this area.

Apple's macOS operating system includes several anti-malware features, including technologies called GateKeeper, XProtect and the Malware Removal Tool (MRT). We explain more about how these work in our blog post, All you need to know about anti-virus on the Mac.

As we explain in **Threat Responses** on page 7, attacks are not usually a single action by a bad guy. They are a series of actions, from the beginning of the attack (such as sending a malicious email), through various stages until the end of the attack, which usually means data theft and/ or destruction. We attempted to follow this full chain of attack, recording if and when the macOS operating system and the anti-malware products detected or stopped us.

We used the default security settings for macOS and, on additional systems, installed the different anti-malware products. We chose those that often appear in reviews and online searches.

In short, the security features of macOS were not sufficient to detect or protect against our attacks. In every case we were able to deliver our malware to the target; run it; gain control; and elevate our access to a very powerful level. As a result we could commit acts such as snooping on the Wifi network, clearing logs of our activity, sending personal data back to the internet and encrypting files on the disk.

Clearly a good anti-malware product is needed to protect against targeted attacks.

Of those that we tested, the majority were excellent. All but one detected all of the threats as they arrived on the system. We were unable to gain any meaningful control of the target system.

The same could not be said for **ClamXAV**, which performed poorly, failing to protect against a single attack. It did nothing to stop us gaining remote access and causing damage to the target.

It seemed to be able to detect nearly half of the threats but in fact it only noticed a script that was one small part of the attacks. It did not stop us hacking the target at all, and we were able to steal information even after these detections.

In situations where attackers are taking remote control of your system to steal and damage data, a small detection like this can at least indicate a larger problem. But it doesn't help inform the victim as to the full extent of the harm that is occurring.

The warning here is about marketing claims. It seems that you have to be very careful to read between the lines when choosing a product. **ClamXAV's** website claims that it will "Protect your Mac without slowing it down," and that it will, "Block viruses, adware and Ransomware." It doesn't explicitly mention hacker attacks, but it does claim to protect your files, privacy and to "Keep cyber criminals away."

The concept that macOS is very secure and immune to malware is clearly incorrect, as our results show. However, you can reduce the risks by using a reputable, well-tested anti-malware product. We recommend double-checking that real-time protection is included with whatever you choose, as it's a crucial component of a good security system.

Appendices

Appendix A: Terms Used

Compromised The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.

Blocked The attack was prevented from making any changes to the target.

False Positive When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.

Neutralised The exploit or malware payload ran on the target but was subsequently removed.

Complete Remediation If a security product removes all significant traces of an attack, it has achieved complete remediation.

Target The test system that is protected by a security product.

Threat A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.

Update Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files or requested individually and live over the internet.

Appendix B: FAQs

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

Q We are a customer considering buying or changing our endpoint protection and/ or endpoint detection and response (EDR) product. Can you help?

A Yes, we frequently run private testing for organisations that are considering changing their security products.
Please contact us at info@selabs.uk for more information.

A full methodology for this test is available from our website.

- The test was conducted between 9th July and 31st July 2026.
- All products were configured using default settings, except macOS, which had its Firewall enabled.
- Targeted attacks were selected and verified by SE Labs.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.

Appendix C: Attack Details

Incident No.	Delivery	Execution	Action	Privilege Escalation	Post-Escalation
1	**T1566.003:** Spear Phishing via Service	**T1059.004:** Unix Shell	**T1083:** File and Directory Discovery	**T1543.001:** Launch Agent	**T1552.003:** Bash History
		T1204.002: Malicious File	**T1057:** Process Discovery		**T1070.003:** Clear Command History
		T1078: Valid Accounts	**T1049:** System Network Connections Discovery		**T1555.001:** Keychain
		T1078.001: Default Accounts	**T1654:** Log Enumeration		**T1573.002:** Asymmetric Cryptography
			T1040: Network Sniffing		**T1564.001:** Hidden Files and Directories
			T1087.002: Domain Account		**T1070.006:** Timestomp
			T1016.001: Internet Connection Discovery		**T1070.002:** Clear Linux or Mac System Logs
			T1082: System Information Discovery		**T1564:** Hide Artifacts
					T1041: Exfiltration Over C2 Channel
2	**T1566.003:** Spear Phishing via Service	**T1059.004:** Unix Shell	**T1083:** File and Directory Discovery	**T1543.004:** Launch Daemon	**T1105:** Ingress Tool Transfer
		T1204.001: Malicious Link	**T1057:** Process Discovery		**T1555.001:** Keychain
		T1204: User Execution	**T1033:** System Owner/User Discovery		**T1070.004:** File Deletion
		T1071.001: Web Protocols	**T1049:** System Network Connections Discovery		**T1564:** Hide Artifacts
			T1016.001: Internet Connection Discovery		**T1222.002:** Linux and Mac File and Directory Permissions Modification
			T1082: System Information Discovery		**T1040:** Network Sniffing
			T1016.002: Wi-Fi Discovery		**T1552.004:** Private Keys
			T1082: System Information Discovery		**T1048.002:** Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
3	**T1566.003:** Spear Phishing via Service	**T1059.004:** Unix Shell	**T1083:** File and Directory Discovery	**T1543.001:** Launch Agent	**T1040:** Network Sniffing
		T1204.002: Malicious File	**T1057:** Process Discovery		**T1105:** Ingress Tool Transfer
		T1078.003: Local Accounts	**T1049:** System Network Connections Discovery		**T1555.001:** Keychain
		T1078.002: Domain Accounts	**T1033:** System Owner/User Discovery		**T1573.002:** Asymmetric Cryptography
			T1082: System Information Discovery		**T1222.002:** Linux and Mac File and Directory Permissions Modification
					T1119: Automated Collection
					T1074.001: Local Data Staging
					T1560.001: Archive via Utility
					T1005: Data from Local System
					T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
4	**T1566.003:** Spear Phishing via Service	**T1059.004:** Unix Shell	**T1083:** File and Directory Discovery		**T1647:** Plist File Modification
		T1204.001: Malicious Link	**T1057:** Process Discovery		
		T1036.004: Masquerade Task or Service			
		T1036.005: Match Legitimate Name or Location			
		T1569.001: Launchctl			
		T1129: Shared Modules			

Appendix D: Product Version

Vendor	Product	Build Version (start)	Build Version (end)
Apple	macOS	MacOS Sequoia 15.5	MacOS Sequoia 15.5
Bitdefender	Antivirus for Mac	Agent: 1.7.2 AntiVirus for Mac: 10.3.3	Agent: 1.7.2 AntiVirus for Mac: 10.3.3
Canimaan Software	ClamXAV	3.10.2(11619)	3.10.2(11619)
ESET	Home Security Essential	9.0.6700.0	9.0.6700.0
Gen Digital	Norton 360	26.7.0	26.7.0
TotalAV	Premium	5.12.28 (510)	5.12.28 (510)

SE LABS

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.