Malwarebytes Anti-Exploit
Product Guide

Malwarebytes™

2026

Table of Contents

Get Started

What is Exploit Protection

Learn what is an exploit, why it is important to stop them, and how Malwarebytes Anti-Exploit can protect your Windows device.

What is an exploit?

From Wikipedia: "An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized)."

There are typically three stages involved in a typical vulnerability exploit attack:

1. The exploit triggers a vulnerability through which the attacker is able to run shellcode to bypass the Operating System built-in protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).
2. The exploit shellcode then runs some special instructions called payload.
3. The payload in turn executes a malicious action. Examples of malicious actions can be "download this EXE from the Internet and execute it" or other more advanced types of actions such as opening a reverse shell to the attacker without any EXE files involved. There have been some very stealth malicious actions in the past such as in the example of the FBI exploit of the Tor Browser Bundle in 2013 where the payload simply executed a call-back packet to the FBI's servers which included the exploited PC's Mac address, the Windows hostname and some other basic personally identifiable information.

Traditional antivirus and endpoint security solutions deal mostly with the payload's malicious action when there is an EXE involved. But the protection from exploits offered by traditional solutions starts taking a dive when the payload is something more advanced and/or in earlier stages of the exploit attack.

Why are traditional security solutions not effective against exploit attacks?

Because of the complexity and polymorphism of these attacks there are very few solutions available in the market to tackle these type of problems. Most existing solutions fall short because they were either designed to be reactive, rely on advanced knowledge of the behavior, or are simply too complex for end users to use:

- Blacklisting security applications such as antivirus signatures, web filtering, intrusion detection, and other such technologies require previous knowledge of the malicious code or attack and are not effective enough to protect against newer attacks launched by cyber criminals.
- Generic techniques like static emulation heuristics and run-time behavioral analysis are built upon previous knowledge of malware family traits or features which cyber criminals have become experts in evading.
- Newer techniques on the market such as advanced HIPS, allow-listing or anti-exe and sandboxing, while more effective, are complex to set up by non-technical users, require a very high degree of maintenance or rely too much on the end user to make the correct decision when presented with detection options. In short, they are not install-and-forget.

Which vulnerability exploits does MBAE protect against?

Malwarebytes Anti-Exploit provides advanced security that combats the problem of exploit attacks against software vulnerabilities by effectively "shielding" popular applications and browsers.

When Malwarebytes Anti-Exploit detects a shielded application being exploited it automatically stops the malicious code from executing. Once the malicious code is stopped, it will automatically close the attacked application. We do this for stability as an attacked application might not function properly after experiencing a vulnerability exploit attempt.

Visit the Malwarebytes Anti-Exploit Frequently Asked Questions to learn more.

Enable or disable Malwarebytes Anti-Exploit Protection

Malwarebytes Anti-Exploit's protection layer can be turned on or off. Learn how to do this below.

Turn Anti-Exploit protection off

Option 1:
Right-click on the system tray icon and in the menu that pops up select **Stop Protection**.

Option 2:
Double-click on the system try Icon and when Malwarebytes Anti-Exploit opens you can select **Stop Protection**.

Turn Anti-Exploit protection on

Option 1:
Right-click on the system tray icon and in the menu that pops up select **Stop Protection**.

Option 2:
Double-click on the system try Icon and when Malwarebytes Anti-Exploit opens you can select **Start Protection**.

Protect additional applications

To configure Malwarebytes Anti-Exploit to protect additional applications, see the instructions below.

1. Launch Malwarebytes Anti-Exploit.
2. Click the **Shields** tab.
3. Click **Add Shield**.
4. Enter the following information
   - **Application Name**: A short description or name of the application you are shielding.
   - **Application File Name:** The exact file name of the application you are shielding.
   - **Choose a profile:** Select the type of application you are shielding. If you are unsure, choose **Other**.
5. Click **OK**.
6. Click on the "**x**" to close the program.

Unblock a program

Malwarebytes Anti-Exploit looks for programs who are misbehaving, then blocks them from executing to ensure that your computer's security isn't compromised. If you find that a program that you trust is being blocked by Anti-Exploit, you can use the instructions below to stop Anti-Exploit from blocking that application.

Add items to Exclude list

1. Launch Malwarebytes Anti-Exploit.
2. Click the **Logs** tab.
3. Click the item you wish to Exclude.
4. Only items with the trash-can icon may be excluded.
5. Click **Exclude**.

Troubleshooting

Malwarebytes Anti-Exploit may block Internet Explorer

Some websites may be blocked by Malwarebytes Anti-Exploit while using Internet Explorer because these sites use are using the deprecated Microsoft VBScripting engine.

As a workaround, you can disable this detection technique in Anti-Exploit. See the steps below.

Disable Internet Explorer VB Scripting

1. Launch Anti-Exploit.
2. Click **Settings > Advanced Settings**.
3. Select the **Application Hardening** tab.
4. For the line, **Disable Internet Explorer VB Scripting**, uncheck the option for Browsers.
5. Click **Apply**.