

Antivirus vs. Anti-Malware: Which One Do I Need?

By Panda Security

Published: 2024-09-13 · Archived: 2026-04-05 16:42:30 UTC

Antivirus scans, detects and removes known viruses, while **anti-malware** protects you against all malicious software, including viruses, spyware and ransomware.

Have you ever clicked on a suspicious link only to realize your computer is running sluggishly or bombarded with [pop-up ads](#)? You've likely encountered malware, and you're not alone. [Millions of households](#) face cyberattacks every year, putting personal data and family information at risk. To deal with these attacks, we need robust cybersecurity solutions like antivirus and anti malware, especially when we heavily rely on our devices for everything.

In this blog post, we will draw a thorough comparison of antivirus vs. anti-malware and answer some frequently asked questions (FAQ), helping you decide which one (or both!) is right for your home network.

What Is Antivirus Software?

Antivirus software is a tool that helps you scan, detect and remove viruses. It acts as a shield for your device, protecting it from viruses (a kind of malicious software). Viruses can replicate themselves and spread throughout your computer system, causing damage and stealing information. Think of them like a digital illness — they can corrupt files, disrupt programs and even give hackers access to your personal data.

Modern antivirus programs go beyond identifying basic viruses, such as a [heuristic virus](#), and offer features like:

- Scanning your device for suspicious activity, including emails, downloads and even websites you visit
- Isolating malicious actors or removing them altogether

What Is Anti-Malware Software?

Antivirus software is a strong defense, but it's [not the only weapon](#) in your cybersecurity arsenal. Anti-malware is a type of software that helps you combat a wider range of malware than just viruses. It can be spyware that steals your data, ransomware that locks your files or trojans that disguise themselves as legitimate programs.

Malware protection is a great way to deal with such threats. A good anti-malware software program can help you:

- Identify and remove various malware threats using techniques like signature-based detection (looking for known malware patterns) and behavioral analysis (monitoring programs for suspicious activity)
- Offer real-time protection by constantly scanning your device for new threats

In 2023, **malware attacks soared to 6.06 billion**, a 10% rise compared to 2022.

Source: SonicWall



What Is the Difference Between Antivirus and Anti-Malware?

Both antivirus and anti-malware help you detect malicious software and protect against it, but they are not the same.

Even though “antivirus” sounds like it only fights computer viruses, it actually protects against many [types of malware](#) that are common today. Antivirus and malware protection go hand in hand. Anti-malware goes one step further and focuses on broader, more advanced software threats, such as hidden keyloggers that steal your keystrokes or rootkits that grant attackers near-invisible control over your device.

They complement each other to act as the highest level of defense against malicious software, along with healthy online habits. In short, anti-malware detects more advanced forms of malware, while antivirus defends against traditional, more established threats.

Antivirus	vs.	Anti-malware
<ul style="list-style-type: none">• Protects against viruses• Signature-based detection• Prevents malicious script from running• Can only identify threats it's seen before		<ul style="list-style-type: none">• Protects against malware• Heuristic-based detection• Proactively detects and removes suspicious activity• Can identify threats it's never seen before

What Should Your Antivirus Software Include?

Key indicators of [well-rounded antivirus software](#) include:

- **Real-time scanning:** Background scanning means the program will detect threats as you encounter them.
- **Automatic updates:** Updates target any new forms of malware since installation.
- **Threat removal:** Your software should remove malware, not just detect and block it.
- **User-friendly interface:** It must cater to those who prefer simplicity and want more control.

What to Look for in Anti-Malware Software

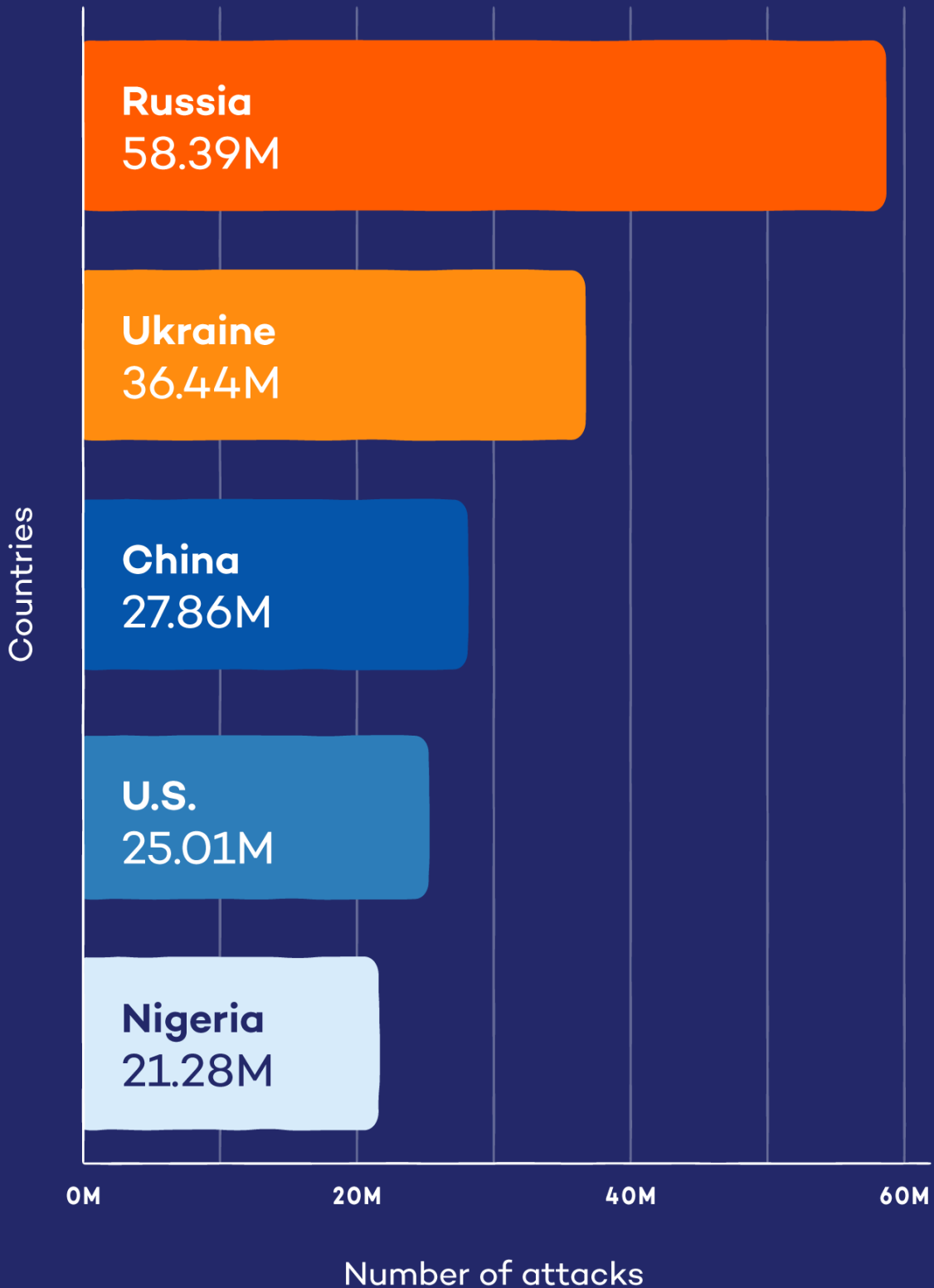
Whether you find separate anti-malware software or purchase antivirus with added capabilities, look for a program with the following:

- **Sandboxing:** This controlled environment allows the software to test suspected threats and determine whether or not they're safe to use.
- **Traffic filtering:** This type of filtering protects your device by blocking access to suspicious servers and sites involved with malware distribution.
- **Proactive security:** Your software should scan, detect and [remove known malware](#) threats like trojans, [adware](#) and spyware.

Do You Need Antivirus or Anti-Malware Software?

Ideally, you'll want both antivirus and anti-malware for the most comprehensive protection. You need antivirus as a strong first line of defense against common threats and anti-malware to tackle a wider range of advanced threats — worms, phishing, [malvertising](#), cryptojacking, botnets and more. They work together to plug security gaps and provide a layered defense against cyberattacks.

World Cybercrime Index (WCI) Score 2024: Top 5 Countries



Source: University of Oxford

As cyberattacks become more prevalent and sophisticated, simply understanding antivirus vs. anti-malware is not enough. You must know all the ins and outs, from antivirus software definition to malware vs. virus. Knowing this information can help you pick the best anti-malware or antivirus software.

Using both antivirus and anti-malware software, along with practicing safe browsing habits, you'll create a layered defense that makes it much harder for malware to infiltrate your device. Consider exploring some popular antivirus options like [Panda Dome](#), specifically made for home users like you so you can protect all your devices, your privacy and your loved ones. You can also check out [Panda Dome's anti-malware](#) for Windows, Mac and Android.

Understanding the nuances of antivirus and anti-malware can be confusing. This FAQ section answers common questions related to both software to help you pick the right defense for your device.

Can I Run Both Antivirus and Anti-Malware Software at the Same Time?

Absolutely! Running both antivirus and anti-malware software is safe and recommended for the most robust defense against cyberthreats. While some resource usage is possible, the benefits of layered protection outweigh the downsides.

Do Antivirus and Anti-Malware Programs Make My Computer Slower?

They can have a slight impact on your computer's performance, but modern software is designed to be efficient.

Which Is More Effective: Antivirus or Anti-Malware?

There's no single winner in this effectiveness battle. Think of it like home security: A deadbolt (antivirus) stops basic break-ins, while an alarm system (anti-malware) deters more sophisticated attempts. Both work together to offer the best defense.

How Do Antivirus and Anti-Spyware Differ?

Antivirus and anti-spyware target different types of threats. Antivirus protects against malicious programs like viruses and worms that can damage or steal data. Anti-spyware specifically targets [spyware](#), a type of malware that monitors your activity and steals personal information like passwords or browsing habits.

Panda Security specializes in the development of endpoint security products and is part of the WatchGuard portfolio of IT security solutions. Initially focused on the development of antivirus software, the company has since expanded its line of business to advanced cyber-security services with technology for preventing cyber-crime.

Source: <https://www.pandasecurity.com/mediacenter/malware/multigrain-malware-pos/>