A

# Antivirus Software: How It Works, What It Detects, and Its Limits

Antivirus software detects, blocks, quarantines, and removes malicious files and behavior. Learn how modern detection works and what protection it cannot provide.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

## In this guide

01 How antivirus software works

02 Real-time protection and on-demand scans

03 Antivirus vs anti-malware

04 What happens after a detection?

05 What antivirus cannot do

06 How to use antivirus effectively

07 Frequently asked questions

**Antivirus software** is a security program that detects, blocks, quarantines, and removes malicious software. Despite the name, a modern antivirus protects against much more than computer viruses: it may identify malware such as Trojans, ransomware, spyware, worms, malicious scripts, and potentially unwanted applications.

Product descriptions and verdicts need separate interpretation. next-generation antivirus describes a set of protection capabilities, while a heuristic virus alert describes how suspicious activity or a file was classified; neither name alone proves a particular infection.

Antivirus reduces risk, but it cannot guarantee that a device will never be compromised. Its effectiveness depends on current detection data, enabled protection, correct configuration, and the behavior of the person using the device.

## 01 How antivirus software works

Modern products combine several detection methods because no single method catches every threat.

| Detection method | What it checks | Main limitation |
|---|---|---|
| Signatures | Looks for code or file patterns associated with known malware. | A completely new or modified sample may not match an existing signature. |
| File reputation | Considers prevalence, age, source, publisher, and cloud intelligence. | New or uncommon legitimate files can appear suspicious. |
| Heuristics | Examines structure and instructions for characteristics common to malware. | Broad rules can produce false positives. |
| Behavior monitoring | Watches running programs for actions such as credential access, persistence, or mass file encryption. | Some activity is visible only after a program starts. |

| Detection method | What it checks | Main limitation |
| --- | --- | --- |
| Machine-learning models | Scores combinations of file and behavioral features. | A score is evidence, not proof; models still require validation and updates. |

A product may also scan web traffic, downloads, email attachments, memory, boot components, scripts, and removable drives. Available layers differ by operating system and product.

## 02 Real-time protection and on-demand scans

- **Real-time or on-access protection** checks files when they are downloaded, opened, created, or executed and monitors active processes.
- **Quick scan** checks common persistence locations, running processes, and other high-risk areas.
- **Full scan** examines a broader set of files and locations and usually takes longer.
- **Custom scan** checks a selected file, folder, drive, or removable device.
- **Offline or boot-time scan** runs before the normal operating environment is fully active, which can help investigate malware that interferes with an ordinary scan.

Real-time protection prevents many threats before execution. An on-demand scan is useful after a suspicious download, unexpected behavior, a missed update, or connection of an untrusted drive.

## 03 Antivirus vs anti-malware

The terms **antivirus** and **anti-malware** now overlap heavily. Historically, antivirus focused on self-replicating viruses while anti-malware described protection against a wider set of threats. Most current products use multiple detection layers and protect against many malware categories, regardless of which term appears in the product name.

Compare actual capabilities rather than assuming one label is broader. Check for real-time monitoring, behavior detection, web protection, ransomware controls, remediation, update frequency, and independent testing.

## 04 What happens after a detection?

1. **Block:** the product prevents a file, connection, or action from continuing.
2. **Quarantine:** it isolates the item so it cannot run normally.
3. **Remediate:** it removes the threat and may reverse related persistence or configuration changes.
4. **Report:** the alert records the detection name, path, process, time, and action taken.

Do not immediately restore an unfamiliar item merely because an application stopped working. Update the antivirus, review the file's source and digital signature, and obtain a second opinion when appropriate. If a trusted file appears to be a false positive, submit it to the relevant security vendor instead of creating a broad exclusion.

## 05 What antivirus cannot do

- It cannot make an unpatched operating system or application safe.
- It cannot prevent a person from voluntarily giving a password or MFA code to a convincing phishing page.
- It may not detect a new exploit, stolen valid account, malicious insider, or attack that leaves few files on disk.
- It cannot recover data when no clean backup exists.
- It cannot replace access control, network segmentation, monitoring, or an incident-response plan.

## 06 How to use antivirus effectively

- Keep the operating system, browser, applications, antivirus engine, and detection data updated.
- Leave real-time and cloud-assisted protection enabled unless a documented troubleshooting step requires a temporary change.
- Use one primary real-time antivirus. Two real-time engines can conflict, duplicate work, or reduce stability.
- Run files from known sources and verify unexpected installers before allowing them through a warning.
- Use unique passwords, phishing-resistant MFA where available, least-privilege accounts, and tested backups.
- Review repeated detections or disabled protection as a possible incident rather than repeatedly dismissing the alert.

## 07 Frequently asked questions

### Do I still need antivirus?

Yes. Built-in or third-party antivirus is one useful layer against malicious code and unsafe downloads. It should operate alongside updates, secure accounts, backups, and careful handling of links and attachments.

### Can antivirus remove every infection?

No. Some compromises require offline scanning, credential rotation, restoration from a known-good backup, or a complete rebuild. If sensitive accounts or business systems may be affected, preserve evidence and involve qualified incident responders.

## Does a clean scan prove a file is safe?

No. A clean result means the scanner did not detect a threat with its current methods and data. Source, signature, behavior, and later reputation still matter.

NEED MORE HELP?

### We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

**Open this guide online at support.gridinsoft.com**