S

Security Software: Types, Limits, and Essential Settings

Security software helps prevent, detect, contain, or recover from threats to devices, accounts, networks, and data. Antivirus is one type; others include firewalls, endpoint detection tools, email filters, and encryption tools. Choose controls for the risks you need to address, keep them working and updated, and check who wil...

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What counts as security software?
02 Main types and their roles
03 What the tools cannot guarantee
04 Essential settings to check
05 Recognizing fake security software
06 How to decide what is sufficient

Quick answer: Security software helps prevent, detect, contain, or recover from threats to devices, accounts, networks, and data. Antivirus is one type; others include firewalls, endpoint detection tools, email filters, and encryption tools. Choose controls for the risks you need to address, keep them working and updated, and check who will respond when they raise an alert.

01 What counts as security software?

The term includes installed programs and cloud services. Some tools block dangerous activity automatically. Others provide evidence for an administrator or help enforce an access policy. A security suite may combine functions, but the feature names alone do not show what is enabled or which devices are covered.

A useful starting point is to name the asset and problem: protecting a stolen laptop's files, detecting malicious code, securing an email account, or recovering deleted documents. These problems require different controls and cannot all be solved by one scan.

02 Main types and their roles

- **Antivirus and anti-malware:** examine files and behavior to detect or block malicious software.
- **Firewalls:** control permitted network connections according to rules.
- **Endpoint detection and response:** collect endpoint activity and support investigation and containment, usually with ongoing administration.
- **Email and web protection:** inspect messages, links, downloads, or destinations for suspicious content.
- **Identity tools:** manage authentication, permissions, and account access.
- **Encryption:** protects data confidentiality under defined conditions, such as a locked device being lost.
- **Backup and recovery tools:** preserve copies and support restoration after deletion or damage.

03 What the tools cannot guarantee

A firewall allowing web traffic does not prove that every page is safe. Encryption does not prevent a signed-in attacker from accessing data through an authorized account. A VPN protects traffic between the device and its endpoint; it does not make a fraudulent website legitimate or remove an infection. Backups restore data but cannot undo information already copied by an intruder.

Likewise, a clean scan is useful evidence, not a guarantee that all accounts and devices are uncompromised. Review the scope of the tool: a program on a computer may have no visibility into a cloud mailbox, router, or phone.

04 Essential settings to check

1. Confirm that the operating system and security application still receive updates.
2. Check that real-time protection and the intended firewall are enabled.
3. Review exclusions and allowed applications; remove obsolete exceptions after verifying their purpose.
4. Confirm that alerts reach a person who knows what action to take.
5. Protect administrative settings and recovery accounts with strong authentication.
6. Check the age and recoverability of important backups.

On managed equipment, coordinate changes with the administrator. Two full antivirus engines running simultaneously can conflict unless their vendors explicitly support that arrangement. An on-demand second-opinion scan is a different use case from two competing real-time engines.

05 Recognizing fake security software

A website claiming to have found hundreds of infections and demanding an immediate payment or phone call is not a trusted device diagnosis. Open the security application independently from the operating system rather than using the page's button. Verify the publisher and download source before installing anything. Do not grant remote control to a person introduced by an

unsolicited warning.

06 How to decide what is sufficient

For a personal device, begin by checking existing protections, account security, automatic updates, and backups. For a business, also consider centralized visibility, staff responsibilities, remote devices, and response capability. A tool that nobody maintains or monitors can leave an important gap despite appearing on a purchasing checklist.

Review protection after a new device, major software change, or incident. Confirm that normal work still functions and that an approved benign test produces the expected notification. Evaluate effectiveness through coverage and response, rather than the number of installed applications.

References: Cisco's overview of security software and Check Point on firewalls and antivirus. Related: defense in depth.

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