

## Anti-malware vs. Antivirus

### Did you know...?

Despite the high popularity of antiviruses, they are estimated to catch **only 45% of attacks**. They are considered highly ineffective nowadays.

Viruses are just one type of malware. Many types of software which can do more damage have recently appeared and spread, for example:



**Adware** – displays ads on the screen of the device, most often in the browser. Adware poses as other applications or hooks up to them, waiting for the installation.



**Spyware** – malicious spyware that secretly observes the actions of the computer user without their consent and reports them to the author of the software.



**Ransomware** – software that blocks/encrypts the device and data, and demands a ransom.



**Rootkit** – software that gives the attacker administrator privileges on the infected operating system.



**Keylogger** – software that records the user's keystrokes on the keyboard and sends them to a hacker who thus receives confidential information, logins, and passwords.

**Cryptojacking** – an attack that allows one to use the computing power of the server/device to mine cryptocurrencies (e.g. bitcoin) for a hacker.

### Fortunately...

**Deep Security Anti-malware** provides protection against any type of malware, using a set of methods: from the malware base, through the verification of known strings/fragments of code, to testing suspicious software with the possibility of rolling back the changes made by this software. It is **the most serious tool providing full protection** against malware.

### And that's not all!

By choosing Deep Security **Malware Prevention** module, apart from professional **Anti-malware**, you also get the **Web Reputation** tool. Trend Micro has one of the largest domain reputation databases, effectively preventing you from visiting an infected or malicious website.