

Antivirus (Antimalware)

Antivirus je software určený k identifikaci, prevenci a odstranění škodlivého kódu ([malwaru](#)), jako jsou viry, trojské koně, červi, spyware nebo [ransomware](#). V moderním pojetí se již častěji setkáme s pojmem **Endpoint Security** nebo **EDR**, protože klasické viry tvoří jen zlomek dnešních hrozeb.

Jak antivirus detekuje hrozby?

Moderní antiviry nepoužívají pouze jednu metodu, ale kombinaci několika přístupů:

1. Signatury (Signature-based)

Antivirus porovnává soubory v počítači s obrovskou databází známých vzorků (otisků) virů.

- **Výhoda:** Extrémně rychlé a přesné u známých hrozeb.
- **Nevýhoda:** Neúčinné proti novým hrozbám ([Zero-day](#)), dokud není databáze aktualizována.

2. Heuristická analýza

Software nehledá přesnou shodu, ale zkoumá kód a hledá podezřelé instrukce typické pro viry (např. pokus o přepsání bootovacího sektoru).

- **Výhoda:** Dokáže odhalit i mírně pozměněné varianty známých virů.

3. Analýza chování (Behavioral Analysis)

Sleduje, co program v systému skutečně dělá. Pokud se legitimně vyhlížejí program náhle pokusí hromadně zašifrovat soubory, antivirus jej zastaví.

- **Výhoda:** Klíčová obrana proti [ransomwaru](#).

4. Cloudová ochrana

Pokud antivirus narazí na neznámý soubor, odešle jeho otisk do cloudu výrobce, kde se okamžitě vyhodnotí na základě dat od milionů jiných uživatelů.

Evoluce: Od Antiviru k EDR

Technologie ochrany koncových bodů se postupem času transformovala:

Typ	Popis
Tradiční Antivirus	Zaměřen na soubory a známé hrozby. Pasivní ochrana.
Next-Gen Antivirus (NGAV)	Využívá strojové učení a AI místo pouhých signatur.
EDR (Endpoint Detection and Response)	Nejen detekuje, ale umožňuje správcům incidenty aktivně vyšetřovat a reagovat na ně v celém podniku.

Klíčové funkce moderního antiviru

- **Rezidentní ochrana:** Běží neustále na pozadí a kontroluje každý soubor, se kterým se pracuje.
- **Kontrola webu:** Blokuje přístup na známé phishingové a podvodné stránky.
- **Ochrana pošty:** Skenuje přílohy e-mailů dříve, než je uživatel otevře.
- **Firewall:** Často bývá součástí balíku pro kontrolu síťového provozu.
- **Sandbox:** Spouštění podezřelých programů v izolovaném „pískovišti“, kde nemohou poškodit systém.

Omezení a rizika

- **Falešný pocit bezpečí:** Žádný antivirus není 100%. Lidský faktor (např. spuštění makra v dokumentu) je stále nejslabším článkem.
- **Zátěž systému:** Náročné skenování může zpomalovat starší počítače.
- **Falešné poplachy (False Positives):** Označení legitimního programu za virus, což může narušit práci.

Doporučení: Pro maximální ochranu v domácím prostředí stačí integrovaný Microsoft Defender, pokud je kombinován s obezřetným chováním. Ve firemním prostředí je standardem nasazení centrálně spravovaného **EDR** řešení.

— **Viz také:** [Ransomware](#), [Zero-day útok](#), [IDS/IPS](#), [Phishing](#)

From:

<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

https://www.serviceit.cz/doku.php?id=it_encyklopedie:malware

Last update: **2026/01/06 17:55**

