NGAV - What it is, how it works, and why it beats legacy AV

Gridinsoft Help Center

NGAV (Next-Generation Antivirus)

What it is

NGAV is a modern security app that stops threats by watching behavior, not just matching virus signatures. It uses heuristics, ML models, and attack-technique rules to block ransomware, fileless attacks, and zero-days. For a deeper look, see our NGAV explainer.

Why it matters

Attackers change code faster than signature updates. NGAV focuses on what attacks do - persistence, credential theft, lateral movement - so it can prevent new variants without waiting for a definition.

How it works - quick tour

- Behavior analytics - flags risky actions like code injection or privilege abuse
- Machine learning - models score files, scripts, and process chains
- Exploit and script control - tames PowerShell, Office macros, LOLBins
- Cloud intelligence - shares indicators to improve protection globally

Where it fits

- Replaces or augments legacy AV on endpoints
- Often paired with EDR/XDR for visibility, hunting, and response
- Useful for remote and hybrid fleets where patch gaps happen

Quick setup tips

- Turn on recommended prevention policies and block mode
- Enforce MFA for console access and lock policy changes to admins
- Enable auto-updates and cloud lookups
- Review alerts weekly, tune noise, and quarantine by default