Host-Based Firewall - What it is, why it matters, and safe default settings

Gridinsoft Help Center

What it is

A host-based firewall runs on a single device and filters that device’s network traffic - blocking suspicious inbound connections and limiting what apps can send out. It’s your last line of defense if something slips past the network edge. For background, see our firewall explainer.

Why it matters

If one laptop gets hit, a host firewall can contain the spread, block lateral movement, and stop malware from calling home.

How it works - quick tour

- Per-app rules - allow or deny network access by program
- Inbound controls - block unsolicited traffic to closed ports
- Outbound controls - stop unknown apps from reaching the internet
- Profiles - different policies for home, work, and public networks

Good uses

- Endpoints on untrusted Wi-Fi
- Servers with limited roles - only required ports open
- Defense in depth with EDR and DNS filtering

Quick setup tips

- Start deny by default for inbound - allow only what you need
- Create per-app outbound rules for sensitive tools
- Turn on logging and review new prompts weekly
- Lock policies with admin rights and use MFA for changes
- Pair with auto-patching and remove unused services