Host-Based IDS - What it is, how it works, and when to use it

Gridinsoft Help Center

What it is

Host-based intrusion detection (often written HIDS) watches a single computer for suspicious activity. It reads system logs, processes, files, and registry changes on that host, then alerts you if behavior breaks policy or matches known attack patterns.

How it works - quick tour

- Sensors on the host collect events like logins, file edits, new services
- Rules and baselines score what is normal vs risky
- Alerting notifies you on tampering, privilege grabs, or malware behavior
- Forensics keeps artifacts for investigation and cleanup

What you may notice

- Alerts about new startup entries or unsigned drivers
- Warnings on sensitive file changes or unexpected admin actions
- Correlation with EDR or SIEM showing the same timeline

Limits to know

- Local overhead - more events mean more CPU and disk
- Noise if rules are too loose - tune to reduce false positives
- Host scope only - it sees that machine, not the whole network

Quick setup tips

- Start with critical servers and high-risk users
- Enable file integrity monitoring on key paths
- Send events to your SIEM and use MFA for console access
- Review and tune rules weekly - suppress known good, tighten high-value detections
- Pair HIDS with network controls and EDR for layered defense