

Honey pot - What it is, why it helps, and smart ways to deploy one

Gridinsoft Help Center

What it is

Why it matters

Real users never touch a honeypot. So any activity you see is suspicious by design - perfect for early warning, threat research, and tuning defenses.

How it works - quick tour

- Decoy assets imitate apps, files, credentials, or services.
- Lures and emulation make it feel authentic to scanners and bots.
- Telemetry captures IPs, tools, commands, and payloads.
- Alerts and blocks feed your SIEM, EDR, and firewall rules.

Good uses

- Early detection: catch brute force, web exploit attempts, and lateral movement.
- Intel gathering: collect indicators to improve blocklists and playbooks.
- Blue-team training: safe space to practice response on real attacker traffic.

Limits to know

- Needs care so it cannot be pivoted into your real network.
- Skilled attackers may probe and spot simple decoys - realism matters.
- Signal volume can rise fast - plan storage and alerting.

Quick setup tips

- Place honeypots in separate VLANs with strict egress rules.
- Seed with believable but fake credentials and data.
- Forward logs to your SIEM and automate IP/domain blocking.
- Review hits weekly and refresh the decoy so it stays convincing.