Defense in Depth (DiD): What it is, why it works, and simple layers to add today

Gridinsoft Help Center

What it is

Defense in Depth is the "many locks, many alarms" approach to security. Instead of betting on one tool, you stack multiple layers - people, process, and technology - so if one layer slips, the next one catches the attack.

Why it matters

Attacks rarely follow one path. A phish might steal a password, then malware moves sideways, then data heads out the door. Layered defenses turn single mistakes into near-misses instead of disasters.

How it works

- Human layer: phishing awareness, safe approvals, reporting culture.
- Identity layer: strong passwords, MFA, least privilege, just-in-time admin.
- Endpoint layer: EDR/AV, patching, disk encryption, device hardening.
- Network layer: segmentation, DNS filtering, firewalls/WAF, DDoS shielding.
- Application/data layer: secure coding, input validation, backups, encryption.
- Monitoring & response: centralized logs, alerts, playbooks, practiced restores.

Quick start

- Turn on MFA everywhere (admins first).
- Patch internet-facing apps fast; remove unused remote access.
- Segment critical systems; block risky egress by default.
- Enable EDR with alerts; log to a central place.
- Keep offline/immutable backups and rehearse a restore.
- Train people to verify money/account changes out of band.

Good to know

- Layers should overlap, not duplicate.
- Balance usability with protection-tune, don’t just pile on.
- Measure results: track time to detect, contain, and recover.