Application Allow-listing: What it is, why it matters, and how to deploy it safely

Gridinsoft Help Center

What it is

Application allow-listing (aka "only these apps may run") is a safety rule for your devices. You create a small, approved list of programs-and everything else is blocked by default. If it’s not on the list, it doesn’t launch.

Why it matters

- Stops malware cold: unknown files can’t execute.
- Shrinks attack surface: fewer ways in, fewer surprises.
- Raises trust: every running app is known and vetted.

How it works (30-second version)

- You approve apps by path, publisher signature, or file hash.
- The system checks each launch against the policy.
- Updates are handled with rules (e.g., allow signed updates from the vendor).

Where it shines

- Servers, admin workstations, POS/kiosks, shared school or library PCs.
- Teams handling sensitive data or high-risk roles.

Gotchas (plan for these)

- Updates break if rules are too strict-build an update path.
- Power users/dev tools may need exceptions or a "developer mode."
- Shadow IT gets surfaced-have a fast request/approval workflow.

Rollout quick plan

- Audit what actually runs (baseline your fleet).
- Draft rules: prefer vendor signature + known paths; hash for high-risk tools.
- Pilot in monitor mode to see blocks without enforcing.
- Enforce gradually; review requests and tune.