Quarantine - what it is, why it helps, and safe restore/remove practices

Gridinsoft Help Center

Quarantine

What it is

Quarantine is a security tool’s safe-hold for suspicious items. Instead of deleting a file outright, the product moves it to a locked location, renames or packages it so it can’t run, and blocks any linked startup hooks. This preserves evidence for review, cuts off execution, and lets you decide to restore (rare), submit for analysis, or remove permanently. It’s different from a sandbox (execution in isolation) and from a recycle bin (simple deletion without containment).

Why it matters

Immediate isolation stops further damage and reduces false-positive risk by giving you a safe review window. It also keeps artifacts for forensics, compliance, and support.

How it works

- Detection -> isolation: File is moved to a restricted folder and rendered non-executable.

- Metadata saved: Original path, hash, detection name, and time are recorded.

- Persistence disabled: Related autoruns (Run keys, tasks, services) are blocked or queued for cleanup.

- Operator choice: Keep for analysis, restore to a test VM, or permanently delete after retention.

What to do

- Review details: original path, detection name, time, and user.

- If the file is business-critical, submit it to your vendor or test in a VM before deciding.

- Do not restore unless you’re confident it’s clean; prefer replacing from a known-good source.

- After backups are verified, delete quarantined items to reduce clutter.

- If credentials or tokens may have been exposed, rotate them even if the file is quarantined.

Watch-outs

- Restoring can re-enable startup entries or scheduled tasks tied to the file. Recheck autoruns after any restore.

- Some threats drop multiple copies; quarantine may catch one while others remain. Run a full scan.

- Quarantine doesn’t undo data theft. If exfiltration is possible, perform account checks and password resets.

- External drives can reintroduce threats. Scan removable media before reconnecting.