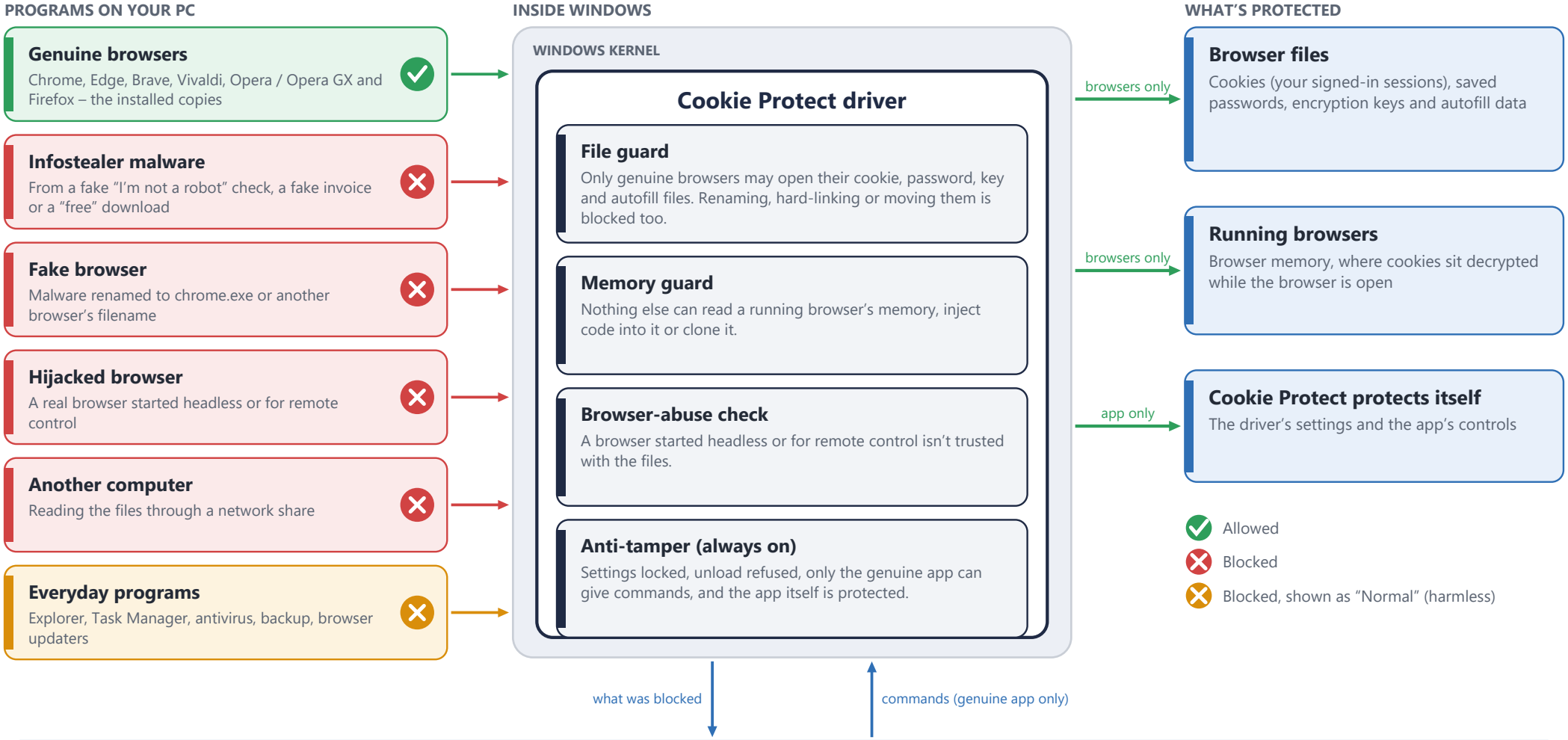
How Cookie Protect works

A small driver inside Windows checks every attempt to open a browser's sensitive files or its memory. Only the genuine, installed browsers get in – everything else is refused and logged.



Cookie Protect app (on your desktop)

Controls
Install the driver, turn protection ON / OFF, Settings switches, Self-Test of every browser.

See what happened
Plain-English Activity lines, e.g. ⚠ BLOCKED: powershell.exe → Chrome cookies, a tray pop-up for real threats, and a coloured status dot.

log.txt
The full record, with origin details for each real threat: program path, what started it, digital signature, SHA-256 fingerprint and a VirusTotal link.

Closing the app doesn't stop protection – the driver keeps blocking. Only the copy of the app that turned protection on can switch it off.

When an infostealer strikes

What happens, step by step

1 The trick
A website shows a fake "I'm not a robot" check and tells you to paste a command into Windows (ClickFix). Or it's a fake invoice or a "free" download.

→

2 Malware runs
A small infostealer starts, running as you. It doesn't need administrator rights – most don't.

→

3 It goes for your logins
Within a second it tries to copy the browser's encryption key, cookies, saved passwords and autofill data.

→

4 The driver checks
"Is this a genuine browser?" No – so Windows answers "access denied". Nothing is read.

→

5 You're told
A ⚠ BLOCKED line in the Activity box, a tray pop-up, and log.txt shows where it came from.

```
⚠ BLOCKED: stealer_demo.exe → Chrome cookies
```

Origin details in log.txt: an unsigned program in the Temp folder, started by PowerShell, started by Explorer – the tell-tale pattern of a pasted command. (Demo example.)

OTHER WAYS IN ARE BLOCKED TOO

Copy tools ✕
cmd, PowerShell, File Explorer, esentutl, robocopy – even as administrator or SYSTEM

Fake browser ✕
Malware renamed to chrome.exe or another browser's filename

Sidestep the file ✕
Renaming, hard-linking or moving the file or the folders it sits in

Another computer ✕
Copying the files through a network share

Browser memory ✕
Reading or injecting into a running browser, or saving a memory dump of it

Clone the browser ✕
Snapshotting a running browser to read the copy

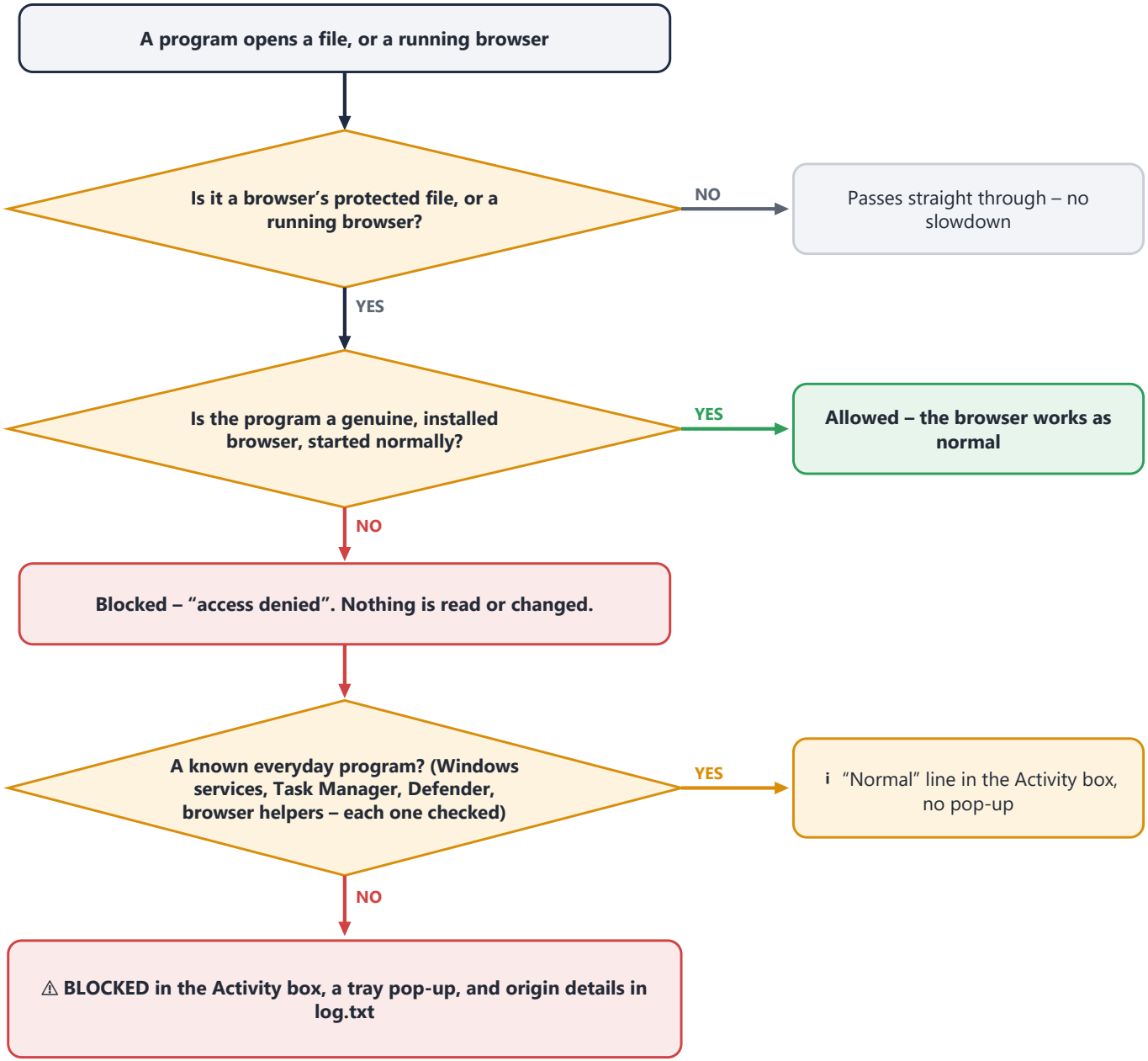
Hijack the browser ✕
Starting it headless or for remote control to pull the cookies out

Switch it off ✕
Unloading the driver, stopping it, or changing its settings

Take over the app ✕
Injecting into the app, or using another copy of it to send commands

The decision – every time

What the driver does with each request



Always on – anti-tamper

- Its settings can't be changed while it runs
- It can't be unloaded or stopped except by the app
- Only the copy of the app that turned it on can give it commands
- Nothing can read or inject into the running app

Good to know

- Closing the app doesn't stop protection
- After a Windows restart, open the app and turn protection ON
- Settings can switch parts off per browser or type of file
- Self-Test checks every browser's files, memory and cloning

Where it works

- Chrome, Edge, Brave, Vivaldi, Opera / Opera GX and Firefox
- 64-bit Windows 10 and 11
- Every profile of each browser

What it doesn't stop

- Malware you've already given full control of the PC
- Someone using your logged-in browser in person
- It's one strong layer – keep your antivirus too