Does turning on my Mac's Firewall give me any additional security? Or do we users have to cofigure the firewall to make it useful?

Turning on macOS's built-in Firewall does give you some protection immediately, even with zero configuration — but it's limited, and understanding what it actually does will help you decide if you need more.

What "just turning it on" gives you

macOS's Firewall (System Settings → Network → Firewall) is an *application-based* firewall, not a traditional port-based one. By default, when you enable it:

- It blocks unsolicited incoming connections to services and apps that aren't explicitly allowed — this stops random network scanners or malware from reaching listening ports on your Mac unprompted.
- Built-in macOS services needed for normal operation (DNS, DHCP, etc.) still work fine.
- Any new app that tries to accept incoming connections will trigger a prompt asking whether to allow or deny it, which gives you some ongoing control without manual setup.

So out of the box, it's already doing useful work: reducing your exposed attack surface from other devices on your network (public Wi-Fi, hotel networks, etc.) trying to probe or connect to your machine.

Where configuration matters more

The default behavior is fairly permissive in one sense: it's designed to avoid breaking things, so:

- Apps you've already approved (or that came signed by Apple) may be allowed automatically without asking.
- It doesn't filter *outgoing* connections at all — if malware is already on your machine phoning home, this firewall won't stop it.
- There's no per-app outbound control, no logging UI by default (you can turn on logging), and no granular rules like a traditional firewall (e.g., pfctl-based).

If you want more control, you can:

- Enable "Firewall Options" → Stealth Mode, which makes your Mac ignore ping/probe requests entirely (harder for scanners to even detect it's there).
- Review and revoke app-level permissions periodically.
- Use a third-party tool (like Little Snitch) if you want outbound filtering — macOS's firewall doesn't do this natively.

Bottom line: turning it on is not just theater — it provides real incoming-connection protection by default. But it's intentionally basic. If your threat model includes wanting to control outbound traffic or lock things down tightly, you'd want additional tools or at least enable Stealth Mode.