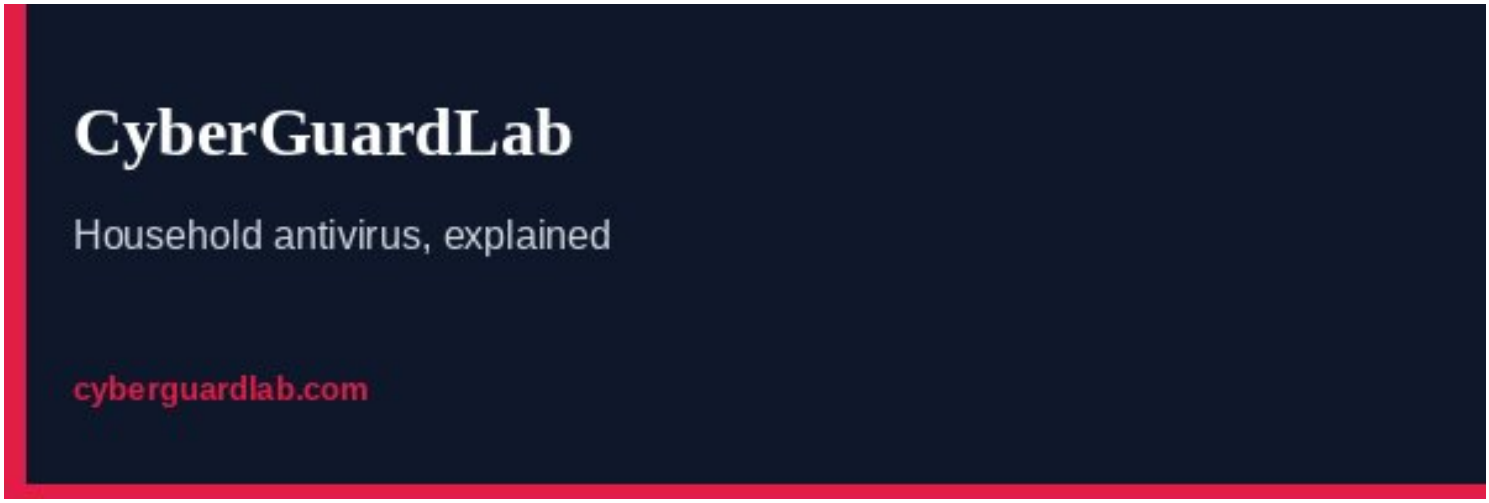
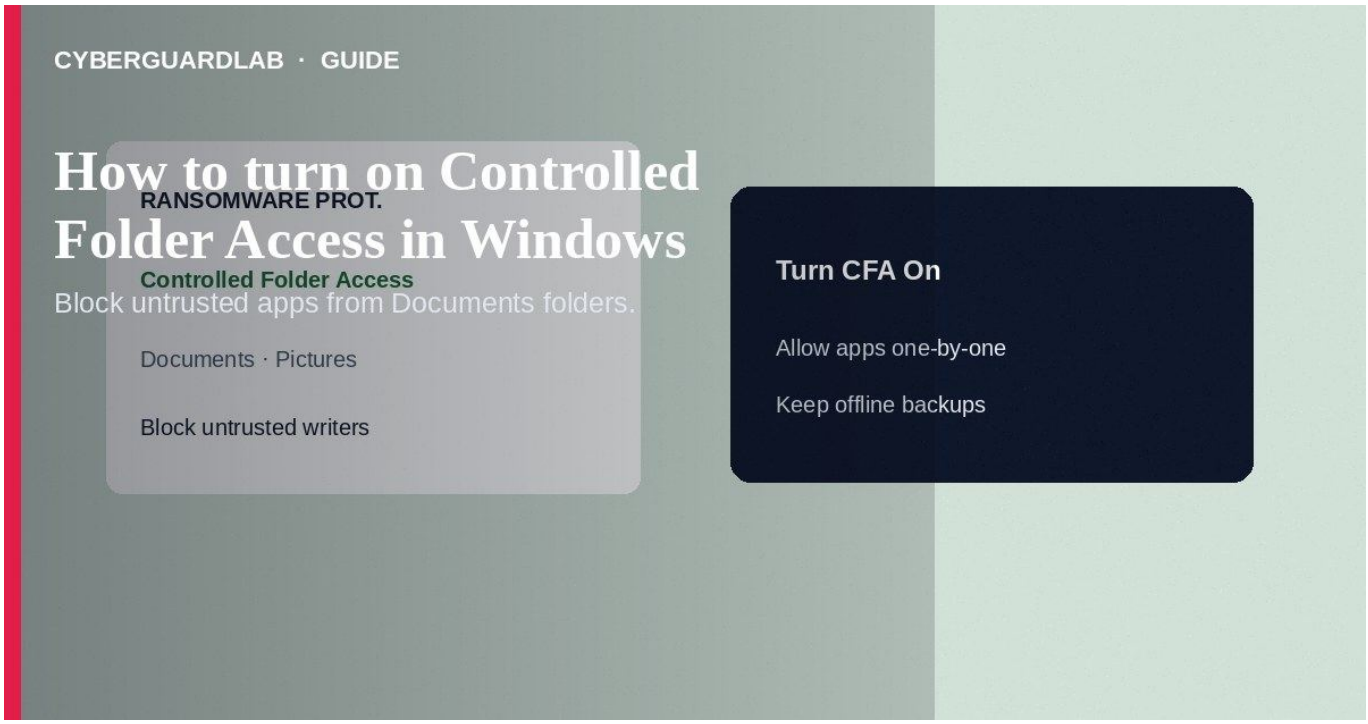


How to turn on Controlled Folder Access in Windows

https://cyberguardlab.com/blog/windows-controlled-folder-access

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



Controlled Folder Access (CFA) in Microsoft Defender Antivirus blocks untrusted apps from changing files in protected folders such as Documents, Pictures, and Desktop-useful ransomware hardening on Windows 10/11. Turn it on in Windows Security under ransomware protection, then allow legitimate apps if they are blocked. This how-to is about CFA-not SmartScreen for apps and files, not core isolation memory integrity, and not reviewing protection history.

1. When CFA helps

Enable CFA on PCs that store irreplaceable local documents and that already run Defender real-time protection. Expect occasional blocks from niche editors, backup tools, or games that write into protected paths-you will whitelist those apps deliberately. CFA is not a substitute for offline backups or for browsing caution.

Paid link

Random posts may tell you to disable CFA or whitelist entire user profiles. Prefer allowing one signed app at a time. If an unknown binary demands access to Documents immediately after a download, delete it-do not allow it.

2. CFA vs neighboring Windows defenses

Feature | Protects against | Where in Windows Security

Controlled Folder Access | Untrusted apps modifying protected folders | Virus & threat -> Ransomware protection

SmartScreen (apps/files) | Unknown/malicious downloads and apps | App & browser control

Memory integrity | Malicious or vulnerable kernel drivers | Device security -> Core isolation

Protection history | (Log) past detections and blocks | Protection history page

3. Steps: turn on Controlled Folder Access

* Open Windows Security (Start -> type Windows Security).
* Go to Virus & threat protection.
* Under Ransomware protection, select Manage ransomware protection (or open Virus & threat protection settings -> Manage Controlled folder access, depending on build).
* Switch Controlled folder access to On. Approve the User Account Control prompt (administrator rights required).
* Confirm Real-time protection is on-CFA depends on Defender's real-time features.
* Optionally select Protected folders and add extra directories that matter (project drives, local vault folders).
* If a trusted app cannot save files, select Allow an app through Controlled folder access -> Add an allowed app and choose the executable.
* Keep monthly backups elsewhere. After malware scares, review blocks and scan with Defender; a trusted third-party tool such as Norton or Bitdefender can be a primary suite instead of stacking multiple full AV products. TotalAV, McAfee, and Avast are other on-site comparison options.

4. If something breaks

* Note which app was blocked (notification or Protection history).
* Allow only executables you recognize from official install paths-not random downloads.
* If ransomware protection shows "No action needed" but you expected CFA on, re-check the toggle and that Defender is active (third-party AV may disable Defender CFA).
* For stubborn false positives, add the folder or app carefully; do not turn CFA off permanently without another backup strategy.

FAQ

Is CFA the same as SmartScreen?

No. SmartScreen reputations check apps/sites you run or visit. CFA restricts file changes inside protected folders even after an app is running.

Do I need administrator rights?

Yes to turn CFA on/off and to manage allowed apps/folders.

Will CFA stop all ransomware?

No single switch does. CFA raises the bar for untrusted writers; keep backups, patching, and careful downloads.

Can I use CFA with a third-party antivirus?

Often Defender CFA is unavailable when another AV owns real-time protection. Follow your suite's ransomware shields instead of stacking conflicting engines.

If you still want a paid suite

Avoiding how to turn on Controlled Folder Access in Windows does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Microsoft Learn: Configure controlled folder access
* Microsoft Support: Protect your files with CFA
* CISA: Protecting against ransomware
* FTC: Computer security

Also read

* How to turn on SmartScreen for apps and files
* How to turn on core isolation memory integrity
* How to check Windows Security protection history
* How to create a Windows local standard user for daily use
* Is Microsoft Defender enough?