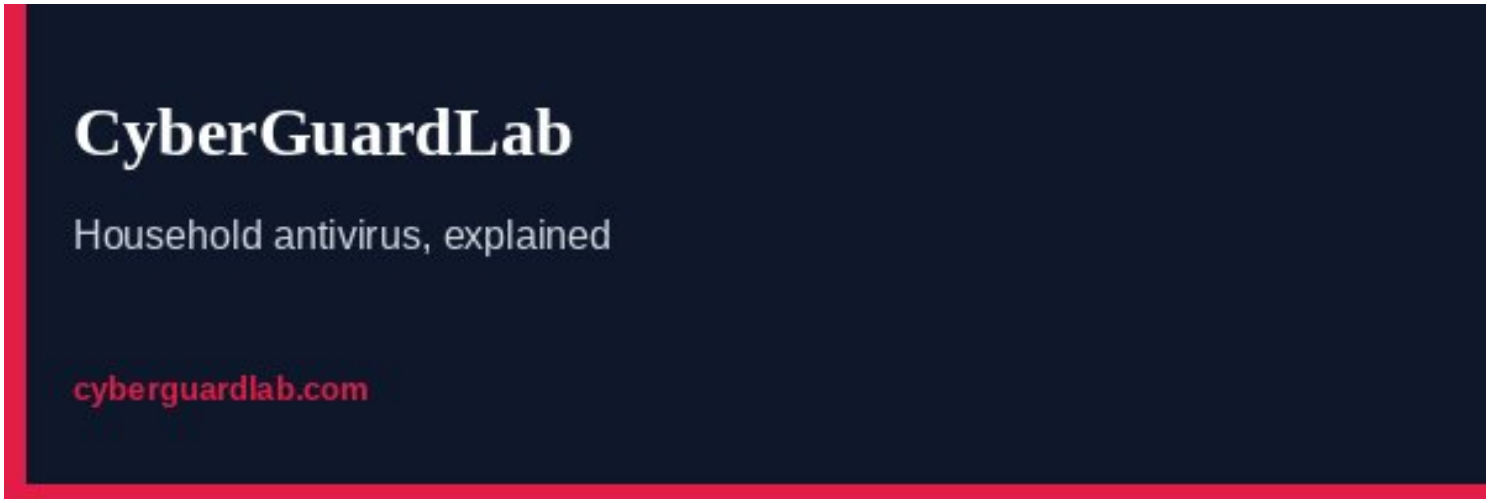
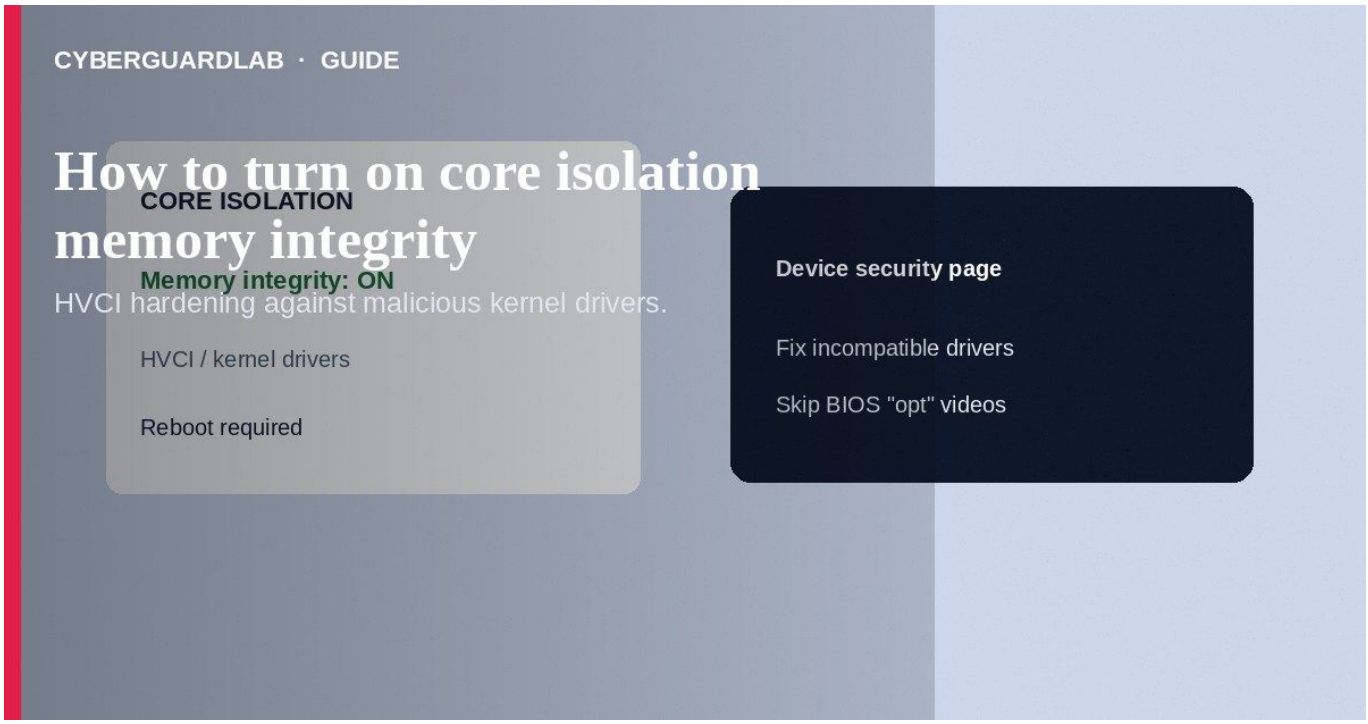


How to turn on core isolation memory integrity

https://cyberguardlab.com/blog/windows-core-isolation-memory-integrity

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.



Memory integrity (also called hypervisor-protected code integrity / HVCI) under Core isolation in Windows Security makes it harder for malicious or vulnerable kernel drivers to tamper with Windows. Turn it on at Device security -> Core isolation details when your PC supports virtualization; update or remove incompatible drivers if the toggle fails. This how-to is about memory integrity-not Controlled Folder Access, not SmartScreen for apps and files, and not Protection history.

1. When memory integrity helps

Enable it on modern Windows 10/11 PCs used for banking, work, and general browsing-especially after Windows warns that memory integrity is off. You need hardware virtualization available in firmware (UEFI/BIOS). Some older anti-cheat or printer drivers conflict; fix drivers rather than leaving the feature off long term when possible.

Paid link

Clickbait guides disable virtualization for a claimed FPS boost and leave memory integrity impossible to enable. Prefer manufacturer documentation when changing firmware. Do not download "one-click BIOS tweakers" from unverified sites.

2. Memory integrity vs other toggles

Feature | Layer | Main job

Memory integrity (HVCI) | Kernel / hypervisor | Protect code integrity from bad drivers

Controlled Folder Access | User files | Stop untrusted apps changing protected folders

SmartScreen apps/files | Application launch | Warn on low-reputation programs

Standard user account | Identity / privilege | Limit standing admin rights

3. Steps: turn on core isolation memory integrity

* Open Windows Security.
* Select Device security.
* Under Core isolation, select Core isolation details.
* Switch Memory integrity to On. Approve UAC if prompted. Restart if Windows asks.
* If the switch will not stay on, open the incompatible driver list Windows shows. Update those drivers from the PC or device maker-or uninstall abandoned devices.
* If virtualization is unavailable, reboot into UEFI/BIOS firmware settings (maker-specific key), enable Intel VT-x / AMD-V / SVM (and related virtualization options your manual names), save, and retry in Windows.
* Confirm Device security no longer warns that memory integrity is off.
* Keep Defender or one trusted suite such as Norton or Bitdefender for malware scanning-memory integrity does not replace antivirus. Avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

4. If a game or device breaks

* Note the exact driver or anti-cheat named in error dialogs.
* Install the vendor's latest Windows-compatible build.
* As a last resort, temporarily turn memory integrity off to finish a critical task, then turn it back on after updates-do not leave it off indefinitely without a reason.
* Prefer replacing ancient USB gadgets that only have unsigned drivers over disabling core isolation forever.

FAQ

Is memory integrity the same as Controlled Folder Access?

No. CFA guards folder writes. Memory integrity hardens kernel code integrity via virtualization-based security.

Will this slow my PC a lot?

Impact varies by hardware. Many modern CPUs run it with modest cost; if performance tanks only in one old app, update that app's drivers first.

Do I need TPM for memory integrity?

Memory integrity relies on virtualization-based security. TPM helps overall platform security posture but follow Microsoft's Device security checklist for your build.

Can a standard user enable it?

The toggle typically requires administrator approval. Enable from an admin account, then return to your daily standard user.

If you still want a paid suite

Avoiding how to turn on core isolation memory integrity 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: Enable memory integrity
* Microsoft Support: Device security in Windows Security
* CISA: Cybersecurity best practices
* FTC: How to secure your computer

Also read

* How to turn on Controlled Folder Access in Windows
* How to turn on SmartScreen for apps and files
* How to check Windows Security protection history
* How to create a Windows local standard user for daily use
* Is Microsoft Defender enough?