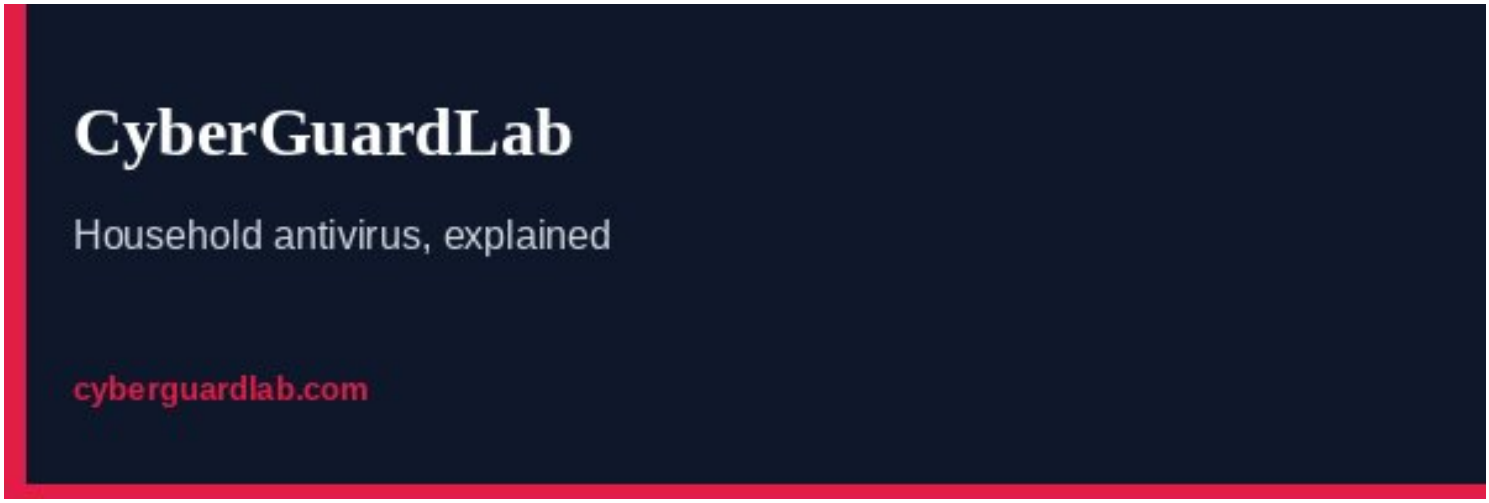
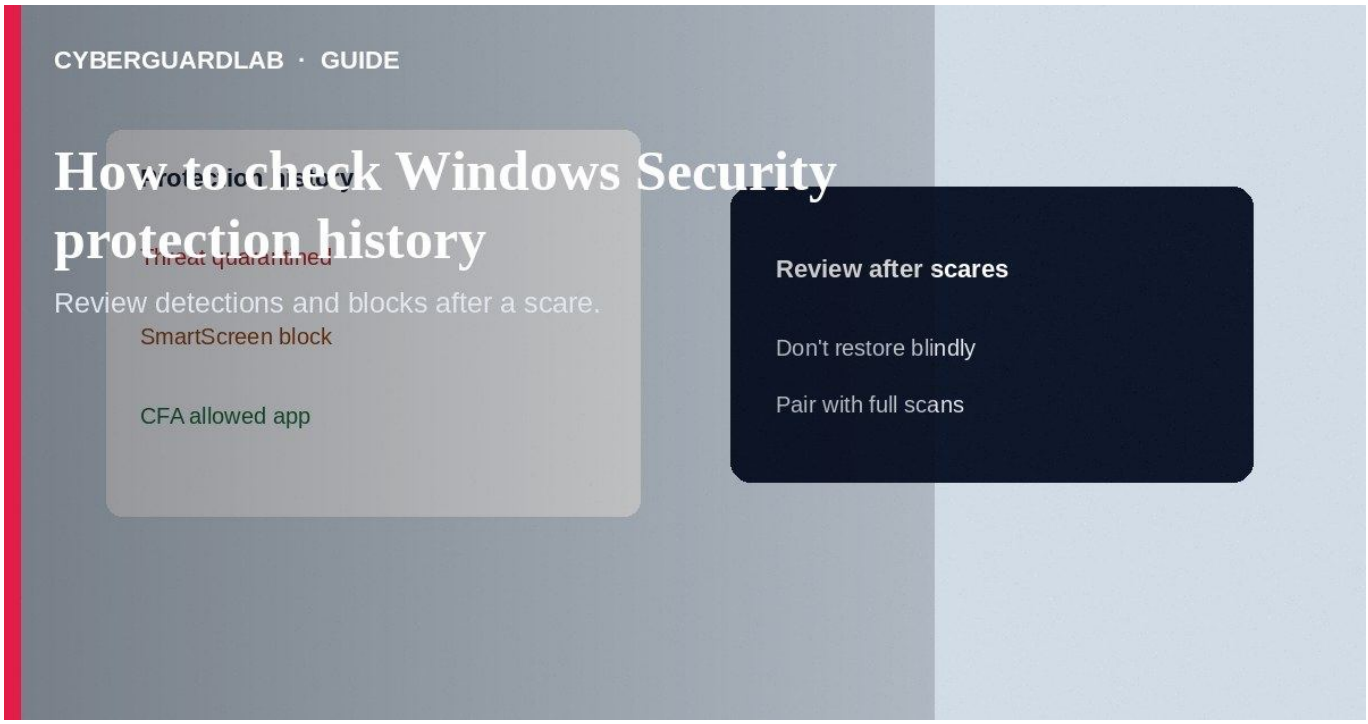


How to check Windows Security protection history

https://cyberguardlab.com/blog/windows-security-protection-history

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.



Windows Security Protection history is the log of recent antivirus detections, SmartScreen blocks, Controlled Folder Access events, and related actions on your PC-use it after a suspicious download, a CFA block, or a scareware pop-up to see what Defender already handled. This how-to is about reading that history-not turning on CFA, SmartScreen, or memory integrity.

1. When to open Protection history

Check it when Windows notified you about a threat, when an app vanished after a scan, when CFA blocked a save, or when you want to confirm a false positive before restoring a file. History is a review tool-it does not by itself enable those protections.

Paid link

Norton 360 | See the Norton first-year offer

Forum posts sometimes tell victims to restore everything so a cracked program runs. That reintroduces malware. Restore only signed, vendor-verified tools-and prefer a clean re-download over quarantine restore when unsure. Open Protection history from the Windows Security app itself so the in-product Help link matches your Windows build.

2. What history shows vs what it is not

You see in history | Configure elsewhere

Past malware detections and quarantine | Real-time protection toggles

SmartScreen / reputation blocks (when logged) | App & browser control settings

Controlled Folder Access blocks | Ransomware protection allow-list

Actions you already took | Memory integrity (Device security)

3. Steps: view and use Protection history

* Open Windows Security.
* Select Protection history (sometimes listed under Virus & threat protection -> Protection history).
* Review entries by time. Expand an item to see severity, affected paths, and actions (quarantined, removed, allowed, blocked).
* Filter or scroll for Blocked, Quarantined, or Allowed items if your build offers filters.
* For a file you believe is safe and was quarantined in error: use the entry's Actions / Restore carefully-only for software you recognize from a vendor you trust.
* For CFA blocks, note the app path; allow it through ransomware protection settings only if legitimate-not from Protection history alone if the UI sends you back to CFA allow-list controls.
* If history is empty but you expected events, confirm real-time protection is on and that a third-party AV has not disabled Defender.
* After restoring anything questionable, run a full scan. Keep one primary real-time antivirus-Defender or a trusted suite such as Norton or Bitdefender. Avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

4. After a serious detection

* Do not restore ransomware or trojan detections "to keep working."
* Change passwords for accounts used on that PC from a clean device if credentials might have been stolen.
* Run an offline Microsoft Defender scan if offered.
* Review startup apps and browser extensions; remove unknowns.
* Report fraud if the detection followed a phishing payment or tech-support scam (ReportFraud.ftc.gov).

FAQ

Is Protection history the same as Controlled Folder Access?

No. History lists events. CFA is the ransomware folder-protection feature that may generate some of those events.

Why can't I see details?

Some views need administrator approval. Sign in with an admin account or approve UAC when prompted.

Does clearing history remove the malware again?

Clearing or aging out log entries does not re-infect you, but it also removes useful forensics-export screenshots before wiping logs if you are investigating.

Will a third-party antivirus show here?

Usually you will see that product's console instead; Defender history may be limited while another AV owns protection.

If you still want a paid suite

Avoiding how to check Windows Security protection history 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 Support: Virus & threat protection in Windows Security
* Microsoft Learn: Microsoft Defender Antivirus on Windows
* Microsoft Support: App & browser control
* FTC: How to secure your computer
* FTC ReportFraud

Also read

* How to turn on Controlled Folder Access in Windows
* How to turn on SmartScreen for apps and files
* How to turn on core isolation memory integrity
* How to create a Windows local standard user for daily use
* How to run a Microsoft Defender offline scan