

Forum: [Hack Forums](#)

Thread: [Anti-malware for Linux](#)

rjusticemi - August 23, 2025, 2:28 pm

Is there any anti-malware program I can use for Linux that uses both heuristic-based detection and signature-based detection? I've known about ClamAV for years, but it's only signature based, so any slightly advanced hacker would easily be able to bypass it by creating polymorphic malware that modifies itself over time. I want something like Bitdefender or MalwareBytes that offers real-time-protection, but I also want the program to be free and open-source.

If you're just gonna respond with something like "anti-malware is not needed on Linux", then just don't reply to this post at all.

Lowkey - August 23, 2025, 2:42 pm

Sophos or Clam AV

Both are worth checking out.

rjusticemi - August 23, 2025, 2:49 pm

(Aug 23, 2025 02:42 PM)Lowkey Wrote: [\[CITE\]](#) Sophos or Clam AV

Both are worth checking out.

You didn't read the post contents; you only read the title. I said in the post that I don't want to use ClamAV because it's only signature-based and is therefore easy to bypass, and Sophos is proprietary/closed-source I think

Lowkey - August 23, 2025, 2:53 pm

(Aug 23, 2025 02:49 PM)rjusticemi Wrote: [\[CITE\]](#) You didn't read the post contents; you only read the title. I said in the post that I don't want to use ClamAV because it's only signature-based and is therefore easy to bypass, and Sophos is proprietary/closed-source I think

You're absolutely right.

Maybe check out eset nod32 then.

DramaKing - August 23, 2025, 2:58 pm

I would say ClamAV, which is still probably the best and most recognizable open-source AV, but I found Kaspersky ES, BitDefender ES, and ESET EA. There's also the open-source Wazuh SIEM.

(Aug 23, 2025 02:53 PM)Lowkey Wrote: [\[CITE\]](#) You're absolutely right.

Maybe check out eset nod32 then.

Still closed-source, but OP is unlikely to get a better option.

ttbr0 - August 23, 2025, 8:08 pm

i dont think this exists. there isnt much incentive to create a complete antivirus solution like for windows. the only exception is for corporate use cases like what elastic edr provides but these are not suitable for the typical home user needs. edrs are supposed to be backed by a blue team that can process and evaluate logs for detection purposes.

it would be interesting to try and write a real time antivirus for linux. i might consider writing something small to play around with and experiment.

MOKO - August 29, 2025, 8:55 am

if you're looking for a free, open-source anti-malware solution for Linux that goes beyond ClamAV's signature-based detection and ventures into heuristic and behavioral analysis, you do have options but unlike the commercial ecosystem, it's often a matter of combining tools into a layered defense.

Linux Malware Detect (LMD) + ClamAV

LMD (a.k.a. Maldet) does heuristic analysis, scanning for behavioral patterns and suspicious file signatures commonly found in shared hosting environments (PHP shells, obfuscated scripts, etc.). When combined with ClamAV, it uses both its own heuristics and ClamAV's AV engine.

Detects polymorphic malware through heuristic rules and regex pattern matching.
Real-time file monitoring supported via inotify (manual configuration required).

Falco (Sysdig OSS Project)

Falco is a runtime security tool that uses syscall monitoring to detect anomalous behavior like:
A non-shell binary spawning a shell
Unexpected file writes
Privilege escalation attempts
Think of it like SELinux, but with real-time anomaly detection, not just policy enforcement.
Behavioral detection at the syscall level
Realtime alerting via stdout, files, or even pushing to SIEM

This is probably the best place to start.

MOKO

HALx86 - September 1, 2025, 10:19 pm

Not antivirus but I know you can set up a pretty gnarly environment using App Armor or SELinux

MadScientist - September 3, 2025, 5:02 am

I think you'd have to combined tools like Snort + ClamAV and such then configure monitor and go over logs manually aside from commercial solutions.

Curious to follow this convo.