ENDOR LABS

Proactive Protection from Malware Attacks

Software supply chain attacks are increasing

Malware in open source dependencies is a fast-growing threat facing application security and engineering teams. The industry has observed a **1,300% increase in malware campaigns since 2023,** primarily targeting registries like npm and PyPI given their popularity and dependency-rich ecosystems.[1]

By the Numbers

18.000
malicious open-source packages were identified by security researchers in Q1 2025[2]

80%
of DevOps teams have delayed CI pipelines due to critical security issues[1]

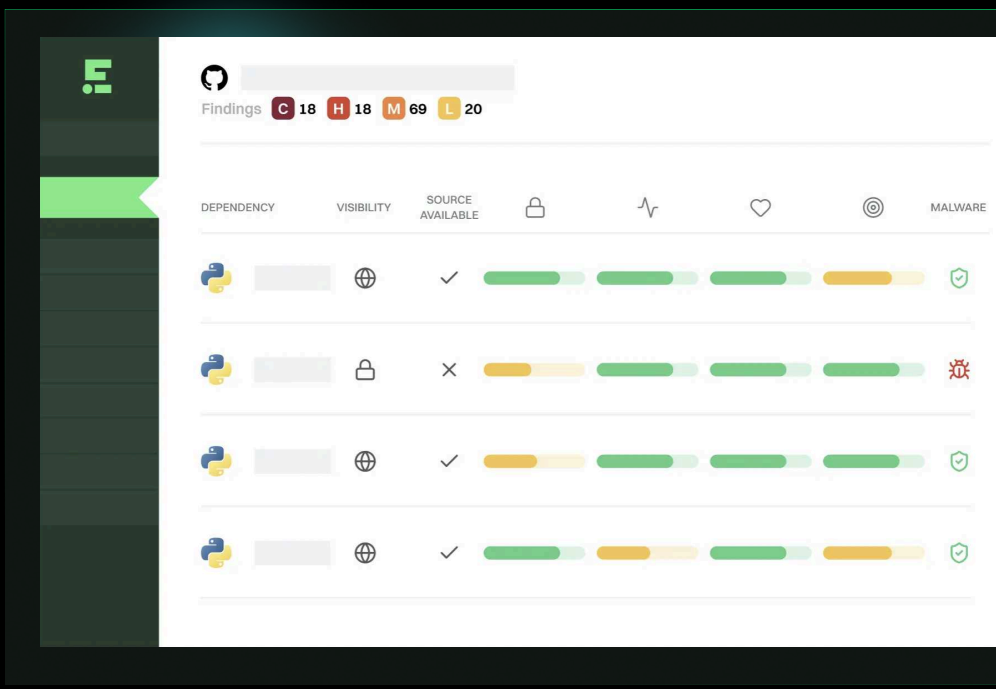
100,000 +
downstream packages on average rely on a popular npm package[3]

Malware campaigns typically burn out quickly but can still have major impacts. Security teams must run rapid incident responses to verify whether environments were impacted, disrupting regular work and delaying releases.

Detect and block malware at the source

While malware risk management seems more reactive than CVE remediation programs, there are many proactive steps you can take.

Endor Labs helps security teams build lasting programs that block malware early, enforce guardrails in development, and reduce incident response workloads.



[1] Software supply chain security by the numbers: 30 stats that matter (Security Boulevard)
[2] Security researchers warn of 18,000 open source malware packages (InfoWorld)
[3] A study of The Security Threats in the npm ecosystem (Proceedings of the 28th USENIX Security Symposium)

Trusted by Security Leaders

> Endor Labs catches malicious dependencies before we even hear about them. Their security research team goes beyond automated detection to help us verify the threat so we can act early and decisively."

Aman Sirohi, SVP
Chief Security Office & Platform @ People.ai

Integrate security into AI-native development

- **Block known malware:** Block known malicious packages from entering your codebase.
- **Identify suspicious behavior:** Scan every package for suspicious code and flags risks such as typosquatting, dependency confusion, and hidden scripts.
- **Expert verification:** The Endor Labs security research team reviews suspicious findings, escalating and notifying you when malware is detected.

Detect design flaws traditional tools can't see

- **Detect unpinned dependencies:** Prevent developers and CI tools from pulling new versions that may contain malware.
- **Enforce mandatory cooldown periods:** Most attacks are resolved in 24-48 hours so simply waiting to adopt new versions is a strong control.
- **Identify unused dependencies:** Reduce your attack surface by eliminating unmaintained or forgotten code that could be exploited.

Get the context you need to act with confidence

- **Review dependencies:** Assesses every open source package against 150+ health checks.
- **Flag weak security practices:** Spot unsafe security practices in project repositories.
- **Identify risky activity:** Flag projects with single maintainers or abandoned projects.

Build a proactive malware prevention program

Book a demo today and learn how Endor Labs can help secure your software supply chain.

endorlabs.com/demo-request