PENTESTERRA

DevGuard

Eliminate security breach risks in your modern development environment that even the best repo scanners don't catch

DEVELOPER-SIDE SECURITY

NO CODE LEAVES THE MACHINE

The Gap No One Is Closing

Most breaches don't start in the repository. They start on the developer's machine — before the first commit.

> Pentesterra DevGuard is a security layer that runs on the developer's machine before every push, catching secrets, malicious packages, and risky AI tooling long before they reach your repositories or production systems.

- No code leaves the machine
- No pipeline bottleneck
- Scans only when you run it

Why Your Development Infrastructure Needs It

Your real attack surface starts on laptops

Credentials in shell history, .env files, AI tools, and IDE plugins are invisible to your existing scanners — but they're exactly what attackers harvest first.

AI coding tools quietly changed your risk profile

MCP servers, AI IDE extensions, and agent frameworks now see your schemas, keys, and internal URLs. One malicious plugin means a supply-chain incident.

You must prove security without sharing your code

In outsourced, regulated, or NDA-heavy environments, security needs visibility while legal and clients say "no code offsite."

One leaked token can cost more than your entire security budget

A single active Stripe, AWS, or GitHub key with wide blast radius can translate into a multi-million-euro breach and regulatory exposure.

What DevGuard Actually Does

Run it before you push. It takes minutes. DevGuard scans the **developer environment** — not just code patterns, but live risk.

Active Secrets

Not "looks like a token." If the token works right now, you know immediately.

AI Tooling Risk

MCP configs, agent permissions, and unsafe extension connections — all surfaced before they become incidents.

Supply-Chain Threats

Malicious packages or hooks already present on the workstation, caught before they ever reach the repo.

High-Risk Code Signals

The things your SAST tool never sees because they never reach CI — risky patterns in code and configuration.

What DevGuard Does *Not* Do

DevGuard is designed to be invisible until you need it. No surprises, no overhead, no vendor lock-in on your source code.

Does not modify your code or environment

It reads. It reports. It never touches your files.

Does not upload your source code anywhere

Everything stays on the machine. Zero data leaves your environment.

Does not run in the background

No antivirus-style daemon consuming resources or watching your every keystroke.

Does not slow down your CI/CD pipeline

You run it when you want to. It reports what it finds. That's it.

DevGuard surfaces risks you currently cannot even see — and turns "I hope nobody leaked a key" into measurable, monitorable facts.

Built to Grow With Your Team

Solo Founder or Early Startup

Get real security coverage from day one — no AppSec hire needed. Free tier, install in minutes. Start protecting your environment before you even have a security team.

Growing Engineering Team (10–50)

Give your tech lead visibility across developers without changing how they work. SOC 2 and enterprise procurement coverage included.

Security-Mature Organization

Org-level enforcement via VCS hooks. Compliance packs and audit trails for regulated industries and enterprise security programs.

Privacy and Your Code Security

Your code and sensitive data **does not leave your machine** — not to LLMs, not to third parties, not even to Pentesterra.

How It Works Locally

01 **DevGuard runs locally using 36+ detection modules**

02 **Before sending telemetry, it masks secrets locally**

Passwords, API keys, tokens, credentials

03 **Only limited evidence is transmitted**

- Masked prefix / fingerprint
- File path + filename
- Package name + version
- What was found / where

This is enough to provide proof and speed up remediation — without exposing the sensitive value itself.

What Is Never Uploaded

- **Source code**
- **Full files**
- **`.env` contents**
- **Clear-text secrets / credentials**

Verify it yourself: `pentesterra-devguard --dry-run` — DevGuard code is not obfuscated. Inspect what it collects.

This is the architectural difference vs many AI coding agents / plugins / scanners:
With them, developers often send code, .env, tokens, and internal context directly into external model pipelines!

With DevGuard:

✅ code stays local ✅ sensitive data stays local ✅ only masked evidence is analyzed

Why Teams Buy It in the First Conversation

> "We adopted AI coding tools and suddenly had no idea what risk that introduced."
> CTO · Series A Startup

> "A credential was committed. We fixed it, but we never want to find out that way again."
> Head of Engineering · Scale-Up

> "Our AppSec tool catches issues in CI. By then it's already too late."
> AppSec Lead · Enterprise

Plans & Pricing

Free

€0 — No card required

- 1 project
- 3 scans/month
- All detection categories
- IDE plugin + CLI
- Install in minutes

Individual

From €23/month

- No limits
- Full findings history
- Priority support

Teams

From €299/month

- Central dashboard
- Org enforcement
- CI/CD integration
- Compliance packs + Audit trails

Close the Gap. Start Today.

Get Started at pentesterra.com/devguard