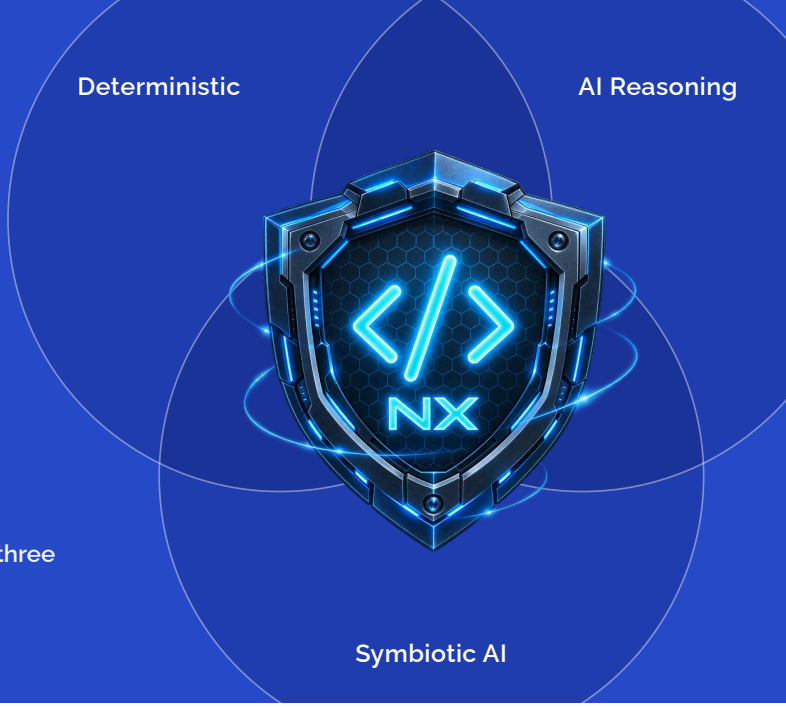
SYHUNT® CODE NX

Product brief **On-device AI**

Find the flaws in your code without sending it anywhere.

Static security testing for web and mobile source code, with three engines and on-device AI.



Your source code is your intellectual property, and every flaw in it is a possible way in. **Syhunt Code NX finds the vulnerable portions of your web and mobile code in minutes**, so they can be patched before release. **All of its AI runs on-device**: inside your own installation, physical or virtual, so the code it analyzes is never sent to an external AI service.

What it changes for you

Source code stays in-house

Code NX reviews your code with AI where it is installed, not in someone else's cloud. **No outside company ever sees your source code**, so protecting your intellectual property and meeting confidentiality commitments stays simple.

Flaws fixed before release

It points developers straight to the vulnerable portions of the code and the key areas to review, and **SurgicalPatch suggests a minimal fix** for each one. Your team stays in control: they review the fix and apply it themselves.

Three engines working together

Syhunt's **proven analysis engine** and **two new AI engines** each examine the code on their own and work together in one scan. Jet-AI **cuts false alarms**, so developers spend their time on real issues.

No AI bills, no new hardware

There are **no per-token fees** for an outside AI service, and Syhunt's **Symbiotic AI** analyzes code on the **ordinary processors you already have**. When a GPU is available, Code NX uses that too, unlocking even more.

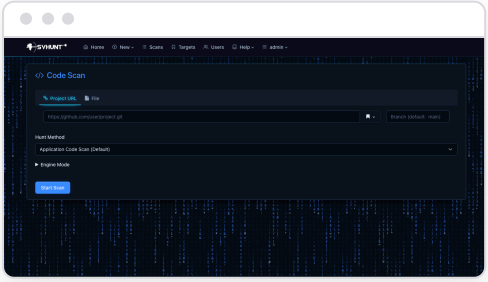
One scanner for web and mobile source code.

1300+ source code vulnerability checks

40+ types of flaws detected

15+ programming languages

Top 10 OWASP web and mobile lists



Start a code scan from a project URL or a file

Fits how your teams work

- Web applications and **Android and iOS apps**, including Android APK analysis.
- Reports with severity scores and compliance mapping for **OWASP Top 10**, **PCI DSS** and CWE/SANS Top 25.
- Works with **GitHub**, **GitLab**, **Bitbucket**, **Jenkins**, **Jira** and more.

Engines, languages, hardware and technical details overleaf

SYHUNT®

www.syhunt.ai

Three engines, working together

Deterministic

Already proven No GPU required

Syhunt's **deep source code analysis** engine. It finds vulnerabilities and highlights key areas of the code for prompt review.

AI Reasoning

New Needs a GPU (RTX)

The **Rea family** of proprietary GenAI models, **Sastria** and **SastriaTwin**: LLMs fine-tuned for SAST, not chat assistants. They settle simple cases quickly and reason step by step through complex ones.

Symbiotic AI

New Runs on CPU, faster on GPU

A Syhunt breakthrough: an analysis engine and an AI model so deeply intertwined that they work only as one. Covers **SAST and MAST**.

Jet-AI Augmentation

New Runs on CPU, faster on GPU

Proprietary fast-decision models that **cut false positives** and take on many additional tasks.

With or without a GPU

	CPU	GPU (RTX)
Symbiotic AI, Jet-AI	Runs	Faster
Deterministic engine	Runs	Not needed
AI Reasoning, SurgicalPatch	Off	**Required**

Minimum and recommended GPU specs will be published in Syhunt's hardware specs.

SurgicalPatch

New Needs a GPU (RTX)

Generates a **minimal patch** for each fix, touching only what is necessary. Code NX only analyzes: you apply the patch yourself.

The Rea and Jet-AI models are **proprietary to Syhunt** and work only inside the product. More Rea models are expected as part of NX.

Web code (SAST)

1300+ vulnerabilities in over 40 types of flaws.

- **ASP.Net (C# & VB.Net), Java (JEE / JSP), JavaScript, Kotlin, Lua, Object Pascal / Delphi, Perl, PHP, Python, Ruby (Rails / ERB) & TypeScript**.
- Supports **MongoDB, Express.js, Angular, AngularJS, Node.js & Koa**, and **Django, mod_python, Python CGI & WSGI**.

AI: Symbiotic AI, Sastria, SastriaTwin, Jet-SAST

Mobile code (MAST)

Top 10 Finds **OWASP Mobile Top 10** vulnerabilities and more.

- **Android & iOS** apps in **Java, Kotlin, Object Pascal (Delphi XE), Objective-C, C, C++ & Swift**, plus **Android APK** analysis.
- Finds flaws such as Insecure Data Storage, Communication, Authentication and Authorization, and Insufficient Cryptography.

AI: Symbiotic AI, Sastria, SastriaTwin, Jet-SAST

Coverage

OWASP Top Ten, PHP Top 5 and other OWASP lists: **XSS, SQL Injection, File Inclusion, Command Execution** and **more**.

17+ database types covered by SQL Injection detection.

Reports

CVSS3 scoring, **CVE / CWE** references and trends over time, with compliance information for OWASP, CWE/SANS Top 25, WASC and **PCI DSS**.

HTML · PDF · JSON · XML · Text · CSV

Integrations

CI and issue tracking

DefectDojo **Faraday** **GitHub**
GitLab **Jenkins** **JIRA**

Virtual bug patching

Imperva **F5 BIG-IP ASM** **ModSecurity**