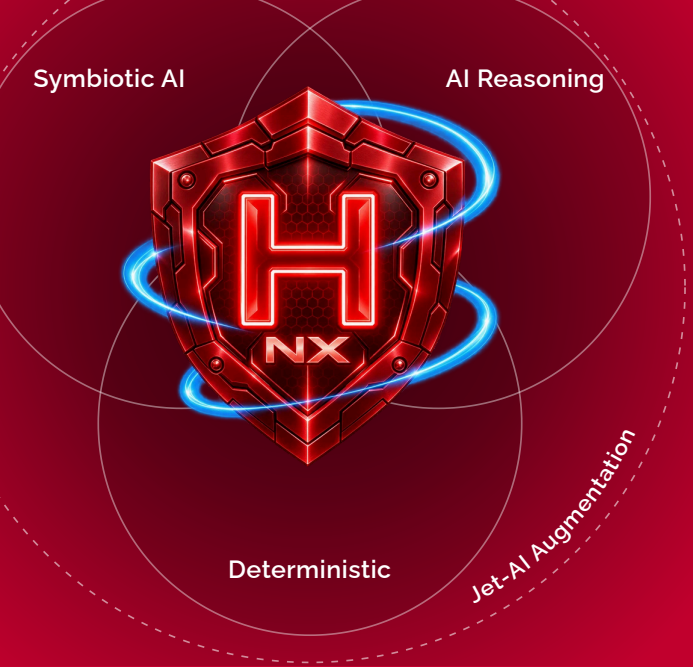


SYHUNT®

HYBRID NX

On-device AI

Product brief

The AI comes to your code. Not the other way around.

Next-generation security testing for web and mobile apps and APIs, with three independent engines and on-device AI.

Most AI security tools send your source code to an external AI service to analyze it. **Syhunt Hybrid NX does the opposite: all of its AI runs on-device**, inside your own installation, physical or virtual. It finds the security flaws in your **web** and **mobile** apps and **web APIs**, and helps your team fix them, without your code ever leaving your environment.

Why it matters

Your code stays yours

The AI works where Hybrid NX is installed, not in someone else's cloud. No source code is sent to an external AI service, so there is **no new third party with access to your code** and nothing new to vet for confidentiality or compliance.

Three engines, one consolidated view

Every application can be checked by **three engines that each find vulnerabilities on their own**: two new AI engines and Syhunt's proven classic engine, built on thousands of expert-written checks. Their results are **consolidated into a single view**, and Jet-AI **cuts false alarms**, so your team works on real issues.

From finding to fixing, faster

Knowing about a flaw is only half the job. **SurgicalPatch suggests a minimal fix** for each issue, touching only what is necessary. Your developers stay in control: they review the fix and apply it themselves.

AI without the extra bills

Cloud AI bills per use (tokens); in-house AI usually needs costly GPUs. Hybrid NX avoids both: **no per-token AI bills**, and Syhunt's **Symbiotic AI** runs on the **ordinary processors you already have**. When a GPU is available, it uses that too, unlocking even more.

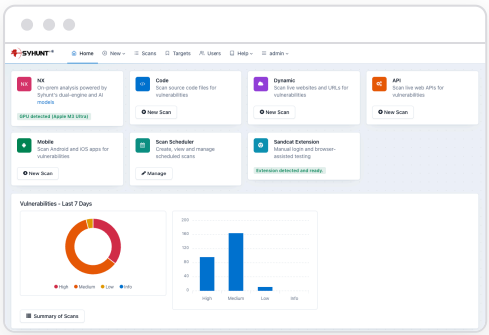
The flaws behind data breaches, found and fixed inside your own walls.

3 independent detection engines

5700+ web application vulnerability checks

1300+ source code vulnerability checks

581+ web API vulnerability checks



The Hybrid NX home screen

Truly hybrid

Four ways of testing, each with deterministic analysis and AI:

Running web apps	DAST	**Source code**	SAST
Mobile apps	MAST	**Web APIs**	AAST

OWASP Top 10 and PCI DSS reports; works with GitHub, GitLab, Bitbucket, Jenkins, Jira and more.

SYHUNT®

Engines, hardware and technical details overleaf

www.syhunt.ai

SYHUNT
HYBRID NX

Technical overview **On-device AI**

Three engines, each detecting vulnerabilities on its own

Symbiotic AI

New Runs on CPU, faster on GPU

A Syhunt breakthrough: an analysis engine and an AI model **fine-tuned for SAST**, so intertwined that they work only as one. Covers **SAST, MAST and SAST-in-DAST**.

AI Reasoning

New Needs a GPU (RTX)

Syhunt's proprietary **Rea** GenAI models, **Sastria** and **SastriaTwin**: LLMs fine-tuned for SAST, not chat assistants. They settle simple cases fast and reason step by step through complex ones, and power **AI-SAST-in-DAST** for client-side JavaScript.

Deterministic

Already proven No GPU required

The engine behind **Syhunt Hybrid**, with **5700+** dynamic and **1300+** code checks. It runs alongside the AI engines, which do not depend on it.

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**

For the minimum and recommended GPU, see Syhunt's hardware specs.

SurgicalPatch

New Needs a GPU (RTX)

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

Rea, Jet-SAST and Jet-DAST are **proprietary Syhunt models**. More Rea models are expected as part of NX.

Dynamic testing (DAST)

5700+ web vulnerabilities in 70+ attack categories, incl. **out-of-band**.

- Live web apps in **ASP.NET, Java, JavaScript, Node.js, Lua, Perl, PHP, Python & Ruby**.
- Full penetration test of the web application layer.
- **Deep crawling** with HTML5 and JS support.

AI: SAST-in-DAST, AI-SAST-in-DAST, Jet-DAST

Code testing (SAST, MAST)

1300+ code vulnerabilities in 40+ types of flaws.

- **Web:** ASP.NET, Java, JavaScript, Kotlin, Lua, Perl, PHP, Python, Ruby & TypeScript.
- **Mobile** (Android & iOS): Java, Kotlin, Objective-C, C, C++, Swift & Delphi, plus APK analysis.

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

API testing

581+ API vulnerabilities in 30 categories.

- From **OpenAPI, Swagger, API Blueprint, Postman** and more.
- Optimized for ASP.NET Core, Java, Node.js, PHP, Python & Ruby.

Coverage

OWASP Top 10, API Security Top 10, PHP Top 5 and more, via static and dynamic analysis.

17+ database types covered by SQL Injection detection.

Reports

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

HTML · PDF · JSON · XML · Text · CSV

Integrations

CI and issue tracking

DefectDojo · Faraday · Bitbucket · GitHub · GitLab · Jenkins · Jira Software

Virtual bug patching

Imperva · F5 BIG-IP ASM · modsecurity Open Source Web Application Firewall

For more information about Syhunt, visit

www.syhunt.ai