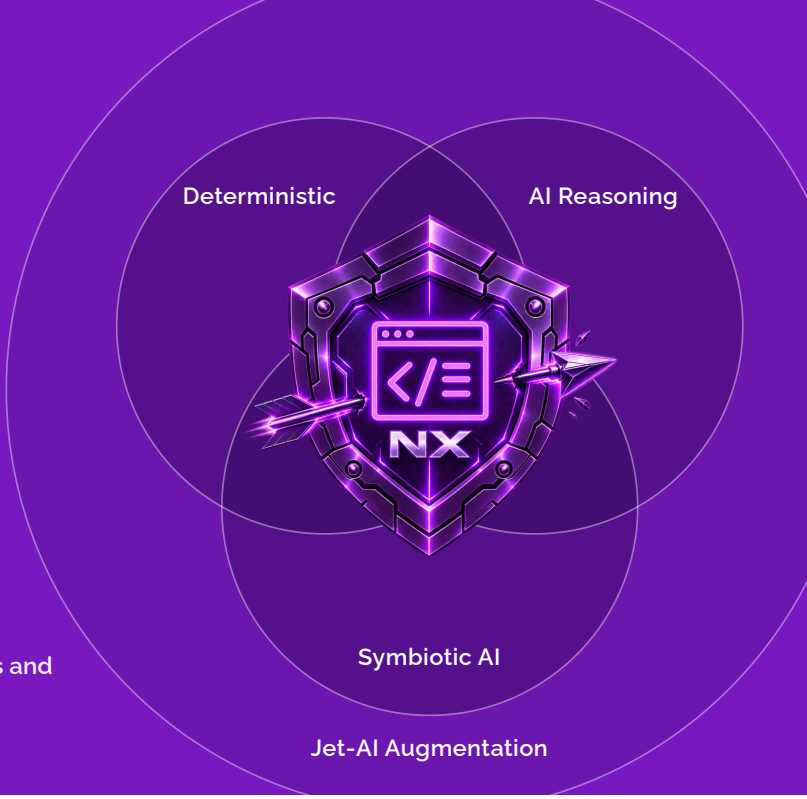
SYHUNT®
# DYNAMIC NX




Product brief **On-device AI**

# Test your web apps and APIs the way attackers do.

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

Attackers don't start with your source code: they probe your running web applications and APIs. **Syhunt Dynamic NX tests them the same way, before attackers do**, including out-of-band attacks that conventional scanners cannot see. **All of its AI runs on-device**, inside your own installation, so the map of your weaknesses it builds never goes to an external AI service.

## What it brings to your business

### Sees what other scanners miss

Out-of-band testing catches **invisible attack variants that conventional dynamic testing cannot detect**, and shows when data can be pulled out of a vulnerable system, with **zero false positives**.

### Testing and code review, in one scan

While it attacks your web apps, its AI also **reviews the JavaScript code they send to every visitor's browser**. Two AI engines do this on their own, alongside Syhunt's proven dynamic engine, and Jet-AI **cuts false alarms**.

### Your weak spots stay private

A list of vulnerabilities is a roadmap for attackers. Dynamic NX analyzes it with AI where it is installed, so **no outside company ever sees your findings** or the code it reviews.

### No AI bills, no new hardware

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

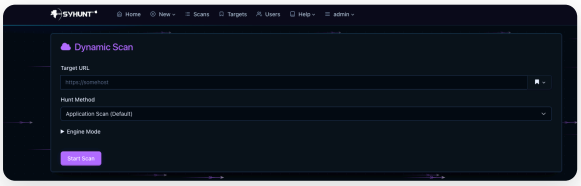
## Your web apps and APIs, tested the way attackers work.

**5700+** web application vulnerability checks

**581+** web API vulnerability checks

**70+** categories of web attacks

**0** false positives in out-of-band tests




Start a dynamic scan from a URL, with a choice of hunt method and engine mode

### From finding to shielding

- Reports mapped to **OWASP Top 10**, OWASP API Top 10 and **PCI DSS**.
- **Virtual patching** with Imperva, F5 BIG-IP ASM and ModSecurity helps shield a flaw until it is fixed.
- Works with **GitHub**, **GitLab**, **Bitbucket**, **Jenkins**, **Jira** and more.

**Engines, out-of-band testing, hardware and technical details overleaf**

SYHUNT®
www.syhunt.ai

# Three engines in one scan

## Deterministic

Already proven · Runs on CPU

Syhunt's dynamic analysis engine. It maps the live web application or API and tests it for **inferential, in-band and out-of-band** attacks.

## 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. In Dynamic NX it covers **SAST-in-DAST**.

## AI Reasoning

New · Needs a GPU (RTX)

The **Rea family** of proprietary GenAI models, **Sastria** and **SastriaTwin**: LLMs fine-tuned for SAST. They power **AI-SAST-in-DAST**, an AI analysis of the client-side JavaScript found during the scan.

## 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** | Off | **Required** |

Minimum and recommended GPU specs will be published in Syhunt's hardware specs. Jet-DAST and the Rea models are proprietary to Syhunt and work only inside the product.

## Out-of-band security testing

Detects invisible, out-of-band variants of attacks that **conventional DAST cannot detect**.

- Listens to forced requests coming from a vulnerable target during the scan.
- Demonstrates data exfiltration from a vulnerable target.
- Returns **zero false positives**.

**Command Execution · SQL Injection · Remote File Inclusion · XXE Injection · Server-Side Request Forgery**

## Web applications (DAST)

**5700+** vulnerabilities in over 70 categories of web attacks.

- Any live web app, especially in **ASP.NET (C# & VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python & Ruby**.
- Complete penetration test of the web application layer, with **deep crawling** and HTML5 and JS support.
- Optimized for sites on **Apache, Tomcat, IIS, Nginx** and more, on Windows, Unix and other platforms.

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

## Web APIs

**581+** API vulnerabilities in 30 categories of web attacks.

- Any web API endpoint, from **API Blueprint, OpenAPI 2/3, Swagger 1/2/3, Postman Collections** and more.
- Complete penetration test of the API, with **fast API crawling** of all endpoints and resources.
- Optimized for **ASP.NET Core (C#), Java (Spring Boot / Jakarta EE), Node.js, PHP, Python & Ruby**.

**AI:** Jet-DAST

## Coverage

OWASP Top Ten, Top 10 API Security Risks, 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

Vulnerabilities and API endpoints, **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** **BitBucket**
**GitHub** **GitLab** **Jenkins**
**JIRA**

Virtual bug patching

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