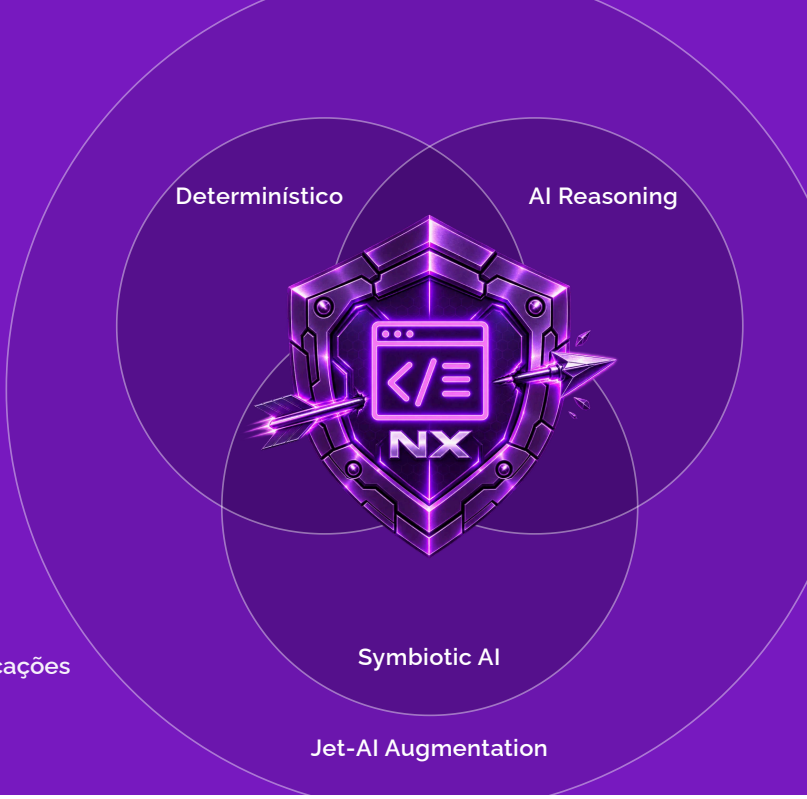
SYHUNT®
DYNAMIC NX



Resumo do produto **IA on-device**

Teste suas aplicações web e APIs como um atacante faria.

Testes de segurança dinâmicos de nova geração para aplicações web e APIs em execução, com três motores e IA on-device.

Atacantes não começam pelo seu código-fonte: eles sondam as suas aplicações web e APIs em execução. **O Syhunt Dynamic NX as testa da mesma forma, antes deles**, incluindo ataques out-of-band que scanners convencionais não enxergam. **Toda a sua IA roda on-device**, na sua própria instalação.

O que ele traz para o seu negócio

Enxerga o que outros não veem

Os testes out-of-band detectam **variantes invisíveis de ataques que o DAST convencional não detecta** e mostram quando dados podem ser extraídos de um sistema vulnerável, com **zero falsos positivos**.

Teste e revisão de código juntos

Enquanto ataca as suas aplicações, a IA também **revisa o JavaScript que elas enviam ao navegador de cada visitante**. Dois motores de IA fazem isso sozinhos, ao lado do motor dinâmico já comprovado da Syhunt.

Suas fraquezas ficam em sigilo

Uma lista de vulnerabilidades é um mapa para atacantes. O Dynamic NX a analisa com IA onde está instalado: **nenhuma outra empresa vê os seus resultados** nem o código revisado.

IA sem custos extras

IA na nuvem cobra por uso (tokens); IA local costuma exigir placas GPU caras. O Dynamic NX evita os dois: **sem cobrança por token**, e o **Symbiotic AI** roda nos **processadores comuns que você já tem**. Com GPU disponível, a solução também a explora e destrava ainda mais recursos.

Suas aplicações web e APIs, testadas como um atacante faria.

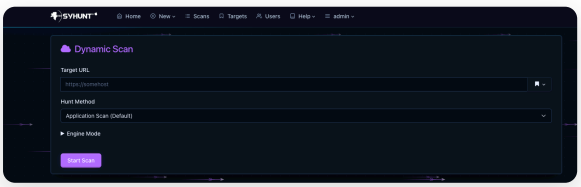
Reforça as medidas de segurança exigidas pela **LGPD**, sem que os seus dados saiam do seu ambiente.

5700+ verificações de aplicações web

581+ verificações de APIs web

70+ categorias de ataques web

0 falsos positivos nos testes out-of-band



Varredura dinâmica a partir de uma URL

Da descoberta à proteção

- Relatórios para **OWASP Top 10**, OWASP API Top 10 e **PCI DSS**.
- **Correção virtual** com Imperva, F5 BIG-IP ASM e ModSecurity protege a falha até a correção.
- Integra-se com **GitHub**, **GitLab**, **Bitbucket**, **Jenkins**, **Jira** e mais.

Motores, testes out-of-band, hardware e detalhes técnicos no verso

SYHUNT®
www.syhunt.ai

SYHUNT
DYNAMIC NX

Visão técnica **IA on-device**

Três motores em uma única varredura

Determinístico

Já comprovado Roda em CPU

O motor de análise dinâmica da Syhunt. Mapeia a aplicação web ou API em execução e a testa contra ataques **inferenciais, in-band e out-of-band**.

Symbiotic AI

Novo CPU, mais rápido em GPU

Uma inovação da Syhunt: um motor de análise e um modelo de IA tão entrelaçados que só funcionam como um. No Dynamic NX, cobre **SAST-in-DAST**.

AI Reasoning

Novo Requer GPU (RTX)

A **família Rea** de modelos GenAI proprietários, **Sastria** e **SastriaTwin**: LLMs ajustados para SAST. Viabilizam o **AI-SAST-in-DAST**, análise por IA do JavaScript do lado do cliente encontrado na varredura.

Jet-AI Augmentation

Novo CPU, mais rápido em GPU

Modelos proprietários de decisão rápida que **reduzem falsos positivos** e assumem muitas tarefas adicionais.

Com ou sem GPU

	CPU	GPU (RTX)
Symbiotic AI, Jet-AI	Roda	Mais rápido
Motor determinístico	Roda	Dispensável
AI Reasoning	Desligado	**Obrigatória**

As especificações mínimas e recomendadas de GPU serão publicadas nas especificações de hardware da Syhunt. O Jet-DAST e os modelos Rea são proprietários da Syhunt e funcionam apenas dentro do produto.

Testes de segurança out-of-band

Detecta variantes invisíveis, out-of-band, de ataques que **o DAST convencional não detecta**.

- Escuta requisições forçadas vindas de um alvo vulnerável durante a varredura.
- Demonstra a exfiltração de dados de um alvo vulnerável.
- Retorna **zero falsos positivos**.

Execução de Comandos · Injeção de SQL · Inclusão Remota de Arquivos · Injeção de XXE · Server-Side Request Forgery

Aplicações web (DAST)

5700+ vulnerabilidades em mais de 70 categorias de ataques web.

- Qualquer aplicação web em execução, especialmente em **ASP.NET (C# e VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python e Ruby**.
- Teste de intrusão completo da camada de aplicação web, com **deep crawling** e suporte a HTML5 e JS.
- Otimizado para sites em **Apache, Tomcat, IIS, Nginx** e outros, em Windows, Unix e outras plataformas.

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

APIs web

581+ vulnerabilidades de API em 30 categorias de ataques web.

- Qualquer endpoint de API web, a partir de **API Blueprint, OpenAPI 2/3, Swagger 1/2/3, Postman Collections** e outros.
- Teste de intrusão completo da API, com **fast API crawling** de todos os endpoints e recursos.
- Otimizado para **ASP.NET Core (C#), Java (Spring Boot / Jakarta EE), Node.js, PHP, Python e Ruby**.

IA: Jet-DAST

Cobertura

OWASP Top Ten, Top 10 API Security Risks, PHP Top 5 e outras listas da OWASP: **XSS, Injeção de SQL, Inclusão de Arquivos, Execução de Comandos** e **mais**.

17+ tipos de banco de dados cobertos na detecção de Injeção de SQL.

Relatórios

Vulnerabilidades e endpoints de API. Pontuação **CVSS3**, referências **CVE / CWE** e evolução ao longo do tempo, com informações de conformidade para OWASP, CWE/SANS Top 25, WASC e **PCI DSS**.

HTML · PDF · JSON · XML · Texto · CSV

Integrações

CI e rastreamento de issues

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

Correção virtual de falhas

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

Para mais informações sobre a Syhunt, acesse **www.syhunt.ai**