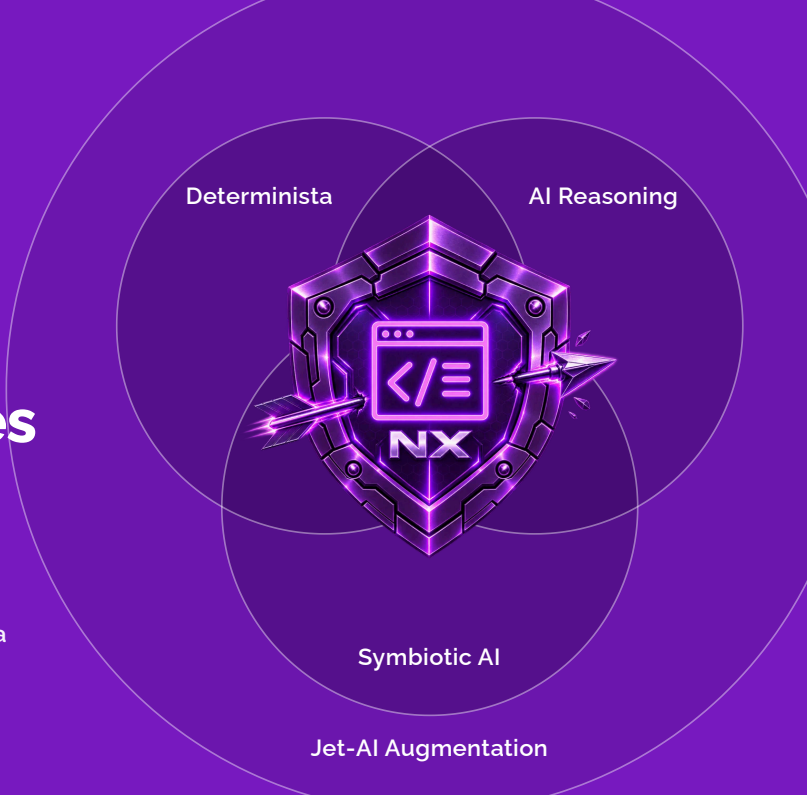
SYHUNT®
# DYNAMIC NX




Resumen del producto **IA on-device**

# Pruebe sus aplicaciones web y APIs como lo haría un atacante.

Pruebas de seguridad dinámicas de nueva generación para aplicaciones web y APIs en ejecución, con tres motores e IA on-device.

Los atacantes no empiezan por su código fuente: sondean sus aplicaciones web y APIs en ejecución. **Syhunt Dynamic NX las prueba de la misma forma, antes que ellos**, incluidos ataques out-of-band que los escáneres convencionales no ven. **Toda su IA se ejecuta on-device**, en su propia instalación.

## Qué aporta a su negocio

### Ve lo que otros no ven

Las pruebas out-of-band detectan **variantes invisibles de ataques que el DAST convencional no detecta** y muestran cuándo se pueden extraer datos de un sistema vulnerable, con **cero falsos positivos**.

### Prueba y revisión de código juntas

Mientras ataca sus aplicaciones, la IA también **revisa el JavaScript que envían al navegador de cada visitante**. Dos motores de IA lo hacen por sí solos, junto al motor dinámico ya probado de Syhunt.

### Sus puntos débiles quedan en privado

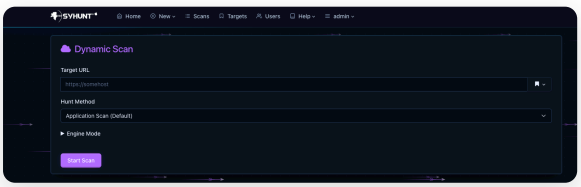
Una lista de vulnerabilidades es un mapa para los atacantes. Dynamic NX la analiza con IA donde está instalado: **ninguna otra empresa ve sus resultados** ni el código revisado.

### IA sin costes extra

La IA en la nube cobra por uso (tokens); la IA local suele exigir GPU caras. Dynamic NX evita ambos: **sin cobro por token**, y **Symbiotic AI** se ejecuta en los **procesadores comunes que usted ya tiene**. Si hay GPU disponible, también la aprovecha y desbloquea aún más funciones.

## Sus aplicaciones web y APIs, probadas como lo haría un atacante.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **5700+** | verificaciones de aplicaciones web | **581+** | verificaciones de APIs web | **70+** | categorías de ataques web | **0** | falsos positivos en pruebas out-of-band |




Escaneo dinámico desde una URL

### Del hallazgo a la protección

- Informes para **OWASP Top 10**, OWASP API Top 10 y **PCI DSS**.
- **Parcheo virtual** con Imperva, F5 BIG-IP ASM y ModSecurity protege el fallo hasta su corrección.
- Se integra con **GitHub**, **GitLab**, **Bitbucket**, **Jenkins**, **Jira** y más.

**Motores, pruebas out-of-band, hardware y detalles técnicos al dorso**

SYHUNT®
www.syhunt.ai

SYHUNT
# DYNAMIC NX

Visión técnica **IA on-device**

## Tres motores en un único escaneo

### Determinista

**Ya probado** Funciona en CPU

El motor de análisis dinámico de Syhunt. Mapea la aplicación web o API en ejecución y la prueba contra ataques **inferenciales, in-band y out-of-band**.

### Symbiotic AI

**Nuevo** CPU, más rápido en GPU

Un avance de Syhunt: un motor de análisis y un modelo de IA tan entrelazados que solo funcionan como uno. En Dynamic NX, cubre **SAST-in-DAST**.

### AI Reasoning

**Nuevo** Requiere GPU (RTX)

La **familia Rea** de modelos GenAI propietarios, **Sastria** y **SastriaTwin**: LLMs ajustados para SAST. Impulsan **AI-SAST-in-DAST**, el análisis por IA del JavaScript del lado del cliente encontrado en el escaneo.

### Jet-AI Augmentation

**Nuevo** CPU, más rápido en GPU

Modelos propietarios de decisión rápida que **reducen los falsos positivos** y asumen muchas tareas adicionales.

### Con o sin GPU

| | CPU | GPU (RTX) |
|---|---|---|
| **Symbiotic AI, Jet-AI** | Funciona | Más rápido |
| **Motor determinista** | Funciona | No necesaria |
| **AI Reasoning** | Apagado | **Obligatoria** |

La GPU mínima y la recomendada se publicarán en las especificaciones de hardware de Syhunt. Jet-DAST y los modelos Rea son propiedad de Syhunt y solo funcionan dentro del producto.

### Pruebas de seguridad out-of-band

Detecta variantes invisibles, out-of-band, de ataques que **el DAST convencional no detecta**.

- Escucha las peticiones forzadas que llegan desde un objetivo vulnerable durante el escaneo.
- Demuestra la exfiltración de datos de un objetivo vulnerable.
- Devuelve **cero falsos positivos**.

**Ejecución de Comandos · Inyección SQL · Inclusión Remota de Archivos · Inyección XXE · Server-Side Request Forgery**

### Aplicaciones web (DAST)

**5700+** vulnerabilidades en más de 70 categorías de ataques web.

- Cualquier aplicación web en ejecución, en especial en **ASP.NET (C# y VB.Net), Java (JEE / JSP), JavaScript, Node.js, Lua, Perl, PHP, Python y Ruby**.
- Prueba de penetración completa de la capa de aplicación web, con **deep crawling** y soporte de HTML5 y JS.
- Optimizado para sitios en **Apache, Tomcat, IIS, Nginx** y otros, en Windows, Unix y otras plataformas.

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

### APIs web

**581+** vulnerabilidades de API en 30 categorías de ataques web.

- Cualquier endpoint de API web, a partir de **API Blueprint, OpenAPI 2/3, Swagger 1/2/3, Postman Collections** y otros.
- Prueba de penetración completa de la API, con **fast API crawling** de todos los endpoints y recursos.
- Optimizado para **ASP.NET Core (C#), Java (Spring Boot / Jakarta EE), Node.js, PHP, Python y Ruby**.

**IA:** Jet-DAST

### Cobertura

OWASP Top Ten, Top 10 API Security Risks, PHP Top 5 y otras listas de OWASP: **XSS, Inyección SQL, Inclusión de Archivos, Ejecución de Comandos** y **más**.

**17+** tipos de bases de datos cubiertos en la detección de Inyección SQL.

### Informes

Vulnerabilidades y endpoints de API. Puntuación **CVSS3**, referencias **CVE / CWE** y evolución a lo largo del tiempo, con información de cumplimiento para OWASP, CWE/SANS Top 25, WASC y **PCI DSS**.

**HTML · PDF · JSON · XML · Texto · CSV**

### Integraciones

CI y seguimiento de incidencias

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

Parcheo virtual de fallos

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

Para más información sobre Syhunt, visite **www.syhunt.ai**