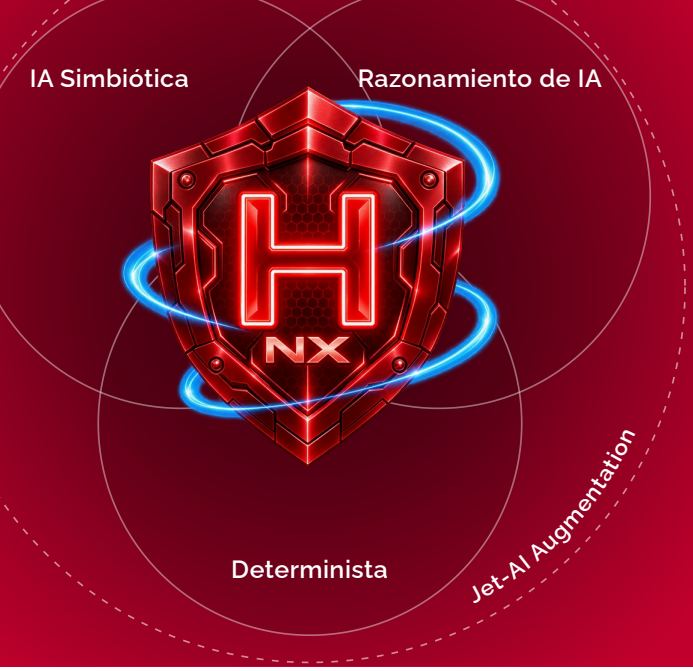


SYHUNT®
HYBRID NX

IA on-device

Resumen del producto

La IA llega a su código. No al revés.

Pruebas de seguridad de nueva generación para apps web y móviles y APIs, con tres motores independientes e IA on-device.

La mayoría de las herramientas de seguridad con IA envían su código fuente a un servicio externo de IA para analizarlo. **Syhunt Hybrid NX hace lo contrario: toda su IA se ejecuta on-device**, dentro de su propia instalación, física o virtual. Encuentra los fallos de seguridad de sus apps **web** y **móviles** y de sus **APIs web**, y ayuda a su equipo a corregirlos, sin que su código salga de su entorno.

Por qué importa

Su código sigue siendo suyo

La IA trabaja donde Hybrid NX está instalado, no en la nube de terceros. Ningún código fuente se envía a un servicio externo de IA: **su código no pasa por las manos de otra empresa**, y usted no crea nuevos riesgos de confidencialidad ni de cumplimiento.

Tres motores, una visión consolidada

Cada aplicación puede ser verificada por **tres motores que encuentran vulnerabilidades por sí solos**: dos nuevos motores de IA y el motor clásico ya probado de Syhunt. Los resultados se **consolidan en una visión única**, y Jet-AI **reduce las falsas alarmas**.

Del hallazgo a la corrección, más rápido

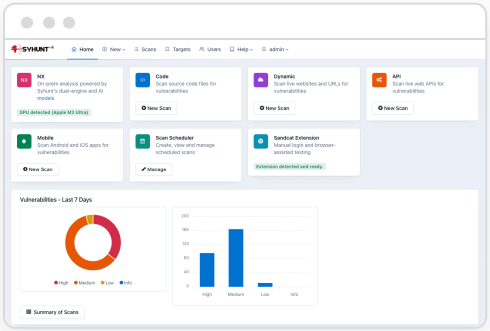
Saber del fallo es solo la mitad del trabajo. **SurgicalPatch sugiere una corrección mínima** para cada problema, tocando solo lo necesario. Sus desarrolladores mantienen el control: ellos revisan y aplican la corrección.

IA sin costes extra

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

Los fallos detrás de las filtraciones de datos, encontrados y corregidos dentro de casa.

3 motores de detección independientes
5700+ verificaciones de vulnerabilidades web
1300+ verificaciones de código fuente
581+ verificaciones de APIs web



La pantalla de inicio de Hybrid NX

Verdaderamente híbrido

Cuatro formas de prueba, cada una con análisis determinista e IA:

Apps web en ejecución	DAST	**Código fuente**	SAST
Apps móviles	MAST	**APIs web**	AAST

Informes OWASP Top 10 y PCI DSS; se integra con GitHub, GitLab, Bitbucket, Jenkins, Jira y más.

SYHUNT®

Motores, hardware y detalles técnicos al dorso

SYHUNT
HYBRID NX

Visión técnica **IA on-device**

Tres motores, cada uno detecta vulnerabilidades por sí solo

IA Simbiótica

Nuevo CPU, acelera con GPU

Un avance de Syhunt: un motor de análisis y un modelo de IA **con ajuste fino para SAST**, tan entrelazados que solo funcionan como uno. Cubre **SAST, MAST y SAST-in-DAST**.

Razonamiento de IA

Nuevo Requiere GPU (RTX)

Los modelos GenAI propietarios **Rea** de Syhunt, **Sastria** y **SastriaTwin**: LLMs con ajuste fino para SAST, no asistentes de chat. Resuelven rápido los casos simples, razonan paso a paso los complejos e impulsan **AI-SAST-in-DAST** para JavaScript client-side.

Determinista

Ya probado No requiere GPU

El motor detrás de **Syhunt Hybrid**, con **5700+** verificaciones dinámicas y **1300+** de código. Se ejecuta junto a los motores de IA, que no dependen de él.

Jet-AI Augmentation

Nuevo CPU, acelera con GPU

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

Con o sin GPU

	CPU	GPU (RTX)
IA Simbiótica, Jet-AI	Funciona	Más rápido
Motor determinista	Funciona	No necesaria
Razonamiento de IA, SurgicalPatch	Apagado	**Obligatoria**

Consulte la GPU mínima y la recomendada en las especificaciones de hardware de Syhunt.

SurgicalPatch

Nuevo Requiere GPU (RTX)

Genera un **parche mínimo** para cada corrección, tocando solo lo necesario. Hybrid NX solo analiza: usted mismo aplica el parche.

Rea, Jet-SAST y Jet-DAST son **modelos propietarios de Syhunt**. Se esperan nuevos modelos Rea como parte de NX.

Pruebas DAST

5700+ vulnerabilidades web en 70+ categorías de ataque, incl. **out-of-band**.

- Apps web en ejecución en **ASP.NET, Java, JavaScript, Node.js, Lua, Perl, PHP, Python y Ruby**.
- Prueba de penetración completa de la capa de aplicación web.
- **Deep crawling** compatible con HTML5 y JS.

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

Pruebas SAST y MAST

1300+ vulnerabilidades de código en 40+ tipos de fallos.

- **Web:** ASP.NET, Java, JavaScript, Kotlin, Lua, Perl, PHP, Python, Ruby y TypeScript.
- **Móvil** (Android e iOS): Java, Kotlin, Objective-C, C, C++, Swift y Delphi, más análisis de APK.

IA: IA Simbiótica, Sastria, SastriaTwin, Jet-SAST

Pruebas de APIs

581+ vulnerabilidades de API en 30 categorías.

- A partir de **OpenAPI, Swagger, API Blueprint, Postman** y más.
- Optimizado para ASP.NET Core, Java, Node.js, PHP, Python y Ruby.

Cobertura

OWASP Top 10, API Security Top 10, PHP Top 5 y más, mediante análisis estático y dinámico.

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

Informes

Puntuación **CVSS3**, referencias **CVE / CWE** y evolución a lo largo del tiempo, con mapeo 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 Software

Parcheo virtual (virtual patching)

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

Para más información sobre Syhunt, visite

www.syhunt.ai