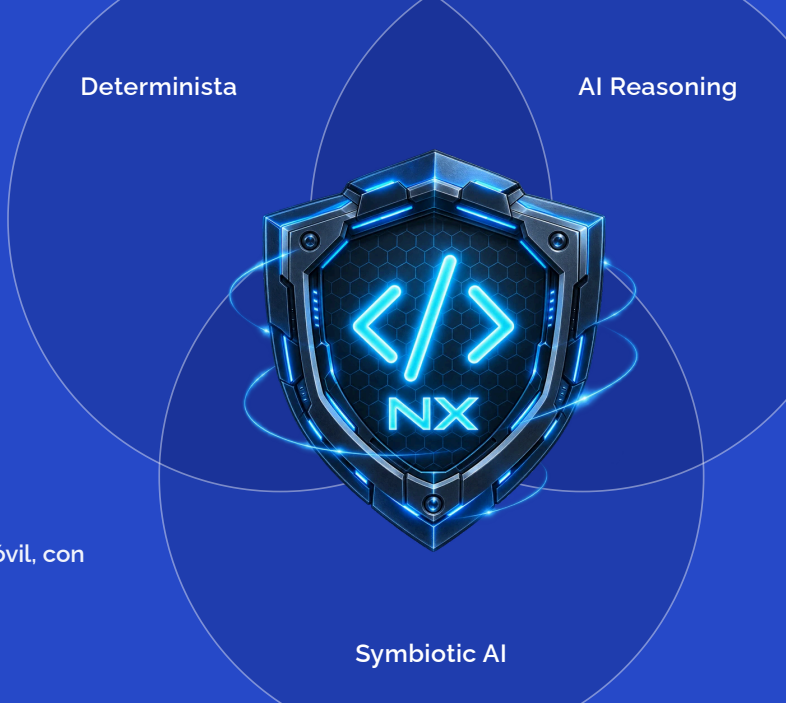
SYHUNT® CODE NX

Resumen del producto **IA on-device**

Encuentre los fallos de su código sin enviarlo a nadie.

Pruebas de seguridad estáticas para código fuente web y móvil, con tres motores e IA on-device.



Su código fuente es propiedad intelectual, y cada fallo en él es una puerta de entrada. **Syhunt Code NX encuentra las partes vulnerables de su código web y móvil en minutos**, para corregirlas antes del lanzamiento. **Toda su IA se ejecuta on-device**: dentro de su propia instalación, física o virtual, sin enviar código a un servicio externo de IA.

Qué cambia para usted

Código fuente dentro de casa

Code NX revisa su código con IA donde está instalado, no en la nube de terceros. **Su código no pasa por las manos de otra empresa**, y proteger su propiedad intelectual sigue siendo sencillo.

Fallos corregidos antes del lanzamiento

Señala a los desarrolladores las partes vulnerables del código y las áreas clave a revisar, y **SurgicalPatch sugiere una corrección mínima** para cada una. El equipo la revisa y la aplica.

Tres motores trabajando juntos

El **motor de análisis ya probado** de Syhunt y **dos nuevos motores de IA** examinan el código, cada uno por sí solo, en un único escaneo. Jet-AI **reduce las falsas alarmas**.

IA sin costes extra

La IA en la nube cobra por uso (tokens); la IA local suele exigir GPU caras. Code 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.

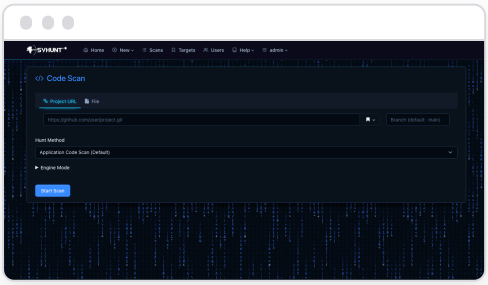
Una sola herramienta para código web y móvil.

1300+ verificaciones de código fuente

40+ tipos de fallos detectados

15+ lenguajes de programación

Top 10 listas OWASP web y móvil



Escaneo desde la URL del proyecto o un archivo

Hecho para el día a día de sus equipos

- Aplicaciones web y **apps Android e iOS**, incluido el análisis de APK de Android.
- Informes con gravedad y cumplimiento para **OWASP Top 10**, **PCI DSS** y CWE/SANS Top 25.
- Se integra con **GitHub**, **GitLab**, **Bitbucket**, **Jenkins**, **Jira** y más.

Motores, lenguajes, hardware y detalles técnicos al dorso

SYHUNT®

www.syhunt.ai

SYHUNT CODE NX

Visión técnica **IA on-device**

Tres motores trabajando juntos

Determinista

Ya probado · No requiere GPU

El motor de **análisis profundo de código fuente** de Syhunt. Encuentra vulnerabilidades y destaca las áreas clave del código para una revisión inmediata.

AI Reasoning

Nuevo · Requiere GPU (RTX)

La **familia Rea** de modelos GenAI propietarios, **Sastria** y **SastriaTwin**: LLMs ajustados para SAST, no asistentes de chat. Resuelven rápido los casos simples y razonan paso a paso los complejos.

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. Cubre **SAST y MAST**.

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, SurgicalPatch	Apagado	**Obligatoria**

La GPU mínima y la recomendada se publicarán en las especificaciones de hardware de Syhunt.

SurgicalPatch

Nuevo · Requiere GPU (RTX)

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

Los modelos Rea y Jet-AI son **propiedad de Syhunt** y solo funcionan dentro del producto. Se esperan nuevos modelos Rea como parte de NX.

Código web (SAST)

1300+ vulnerabilidades en más de 40 tipos de fallos.

- **ASP.Net (C# y VB.Net), Java (JEE / JSP), JavaScript, Kotlin, Lua, Object Pascal / Delphi, Perl, PHP, Python, Ruby (Rails / ERB) y TypeScript**.
- Compatible con **MongoDB, Express.js, Angular, AngularJS, Node.js y Koa**, y con **Django, mod_python, Python CGI y WSGI**.

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

Código móvil (MAST)

Top 10 Encuentra vulnerabilidades del **OWASP Mobile Top 10** y más.

- Apps **Android e iOS** en **Java, Kotlin, Object Pascal (Delphi XE), Objective-C, C, C++ y Swift**, más análisis de **APK de Android**.
- Encuentra fallos como almacenamiento, comunicación, autenticación y autorización inseguros, y criptografía insuficiente.

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

Cobertura

OWASP Top Ten, 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

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** **GitHub**
GitLab **Jenkins** **JIRA**

Parcheo virtual de fallos

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

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