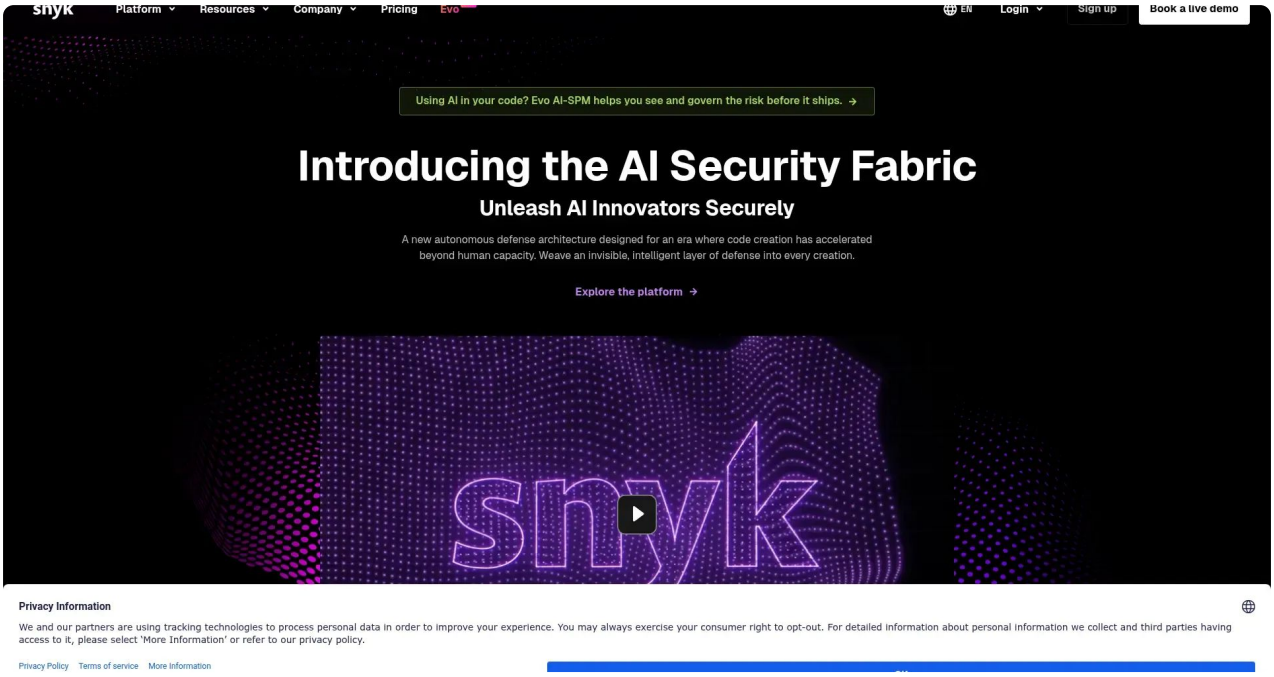

Snyk

Snyk es una plataforma de seguridad líder diseñada específicamente para desarrolladores, ingenieros DevOps y equipos de AppSec que buscan integrar la seguridad en el ciclo de vida del desarrollo de software (SDLC). Permite detectar y corregir automáticamente vulnerabilidades en código propio, dependencias de código abierto, imágenes de contenedores y plantillas de infraestructura como código (IaC). Es la solución ideal para empresas que necesitan mitigar riesgos técnicos sin sacrificar la velocidad de entrega, gracias a su capacidad de generar pull requests automáticos para la remediación de fallos críticos.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Snyk es una plataforma de seguridad diseñada con una mentalidad "developer-first", cuyo objetivo es detectar y corregir vulnerabilidades en el ciclo de vida del desarrollo de software (SDLC). A diferencia de las herramientas de seguridad tradicionales que generan informes para auditores, Snyk se integra directamente en el entorno de trabajo del programador para ofrecer soluciones accionables. Está dirigida a empresas de todos los tamaños (desde startups hasta corporaciones del IBEX 35), departamentos de ingeniería, DevOps y equipos de seguridad (AppSec) que buscan mitigar riesgos sin frenar la velocidad de entrega de código.

Principal ventaja profesional
La capacidad de "auto-remediación": Snyk no solo identifica el problema (CVE), sino que genera automáticamente pull requests (PR) para actualizar dependencias vulnerables a versiones seguras, permitiendo que el desarrollador solucione fallos de seguridad críticos con un solo clic y sin salir de su flujo de trabajo habitual.

Para quién no es
No es apta para organizaciones que no utilicen metodologías de desarrollo moderno (CI/CD) o que operen con tecnologías obsoletas no soportadas por sus escáneres. Profesionales con una mentalidad de seguridad puramente perimetral o auditora, que prefieran revisiones manuales aisladas al final del proyecto, la encontrarán intrusiva o excesivamente automatizada.

Funcionalidades clave
- Snyk Open Source (SCA): Análisis de dependencias de terceros y gestión de cumplimiento de licencias.
- Snyk Code (SAST): Análisis estático de código propio basado en IA para detectar fallos lógicos en tiempo real.
- Snyk Container: Escaneo de imágenes Docker y cargas de trabajo en Kubernetes para detectar vulnerabilidades en el SO y capas base.
- Snyk Infrastructure as Code (IaC): Escaneo de plantillas Terraform, CloudFormation y Kubernetes para evitar configuraciones de nube inseguras.
- Snyk AppRisk: Gestión de la postura de seguridad de las aplicaciones a nivel de inventario y activos de software.
- Base de datos de vulnerabilidades propia: Actualizada con mayor rapidez que la NVD pública.

Precios
- Versión gratuita: Incluye 200 tests de código abierto al mes, 100 de contenedores y 300 de IaC. Es ideal para desarrolladores individuales o proyectos pequeños.
- Team (desde 25€/mes por desarrollador): Para equipos de hasta 10 integrantes. Ofrece tests ilimitados, cumplimiento de licencias e integración con Jira.
- Enterprise (Precio personalizado): Sin límite de usuarios, incluye SSO/SAML, políticas de seguridad personalizadas, acceso a API completa y soporte dedicado.
- Ignite: Pack específico para organizaciones con menos de 50 desarrolladores que requieren funciones Enterprise (aprox. 1.260€/año por desarrollador).

Perfil del usuario
- Empresas tecnológicas y de servicios financieros que priorizan la seguridad técnica.
- Departamentos de Ingeniería de Software y DevOps.
- Perfiles profesionales: Desarrolladores Fullstack/Backend, Ingenieros de Seguridad, SRE (Site Reliability Engineers) y CTOs.

Nivel técnico requerido
- Uso: Medio. El desarrollador solo necesita interpretar las recomendaciones de la herramienta.
- Instalación/Configuración: Medio-Alto. Requiere conocimientos de CI/CD, gestión de repositorios (Git) y configuración de webhooks o CLI.
- Soporte: Requiere coordinación entre el equipo de infraestructura/DevOps para las integraciones iniciales.

Ejemplos de uso profesional
- Automatización del cumplimiento legal: Bloqueo automático de PRs que introduzcan bibliotecas con licencias no permitidas (ej. GPL en productos comerciales).
- Seguridad en el despliegue: Escaneo de contenedores antes de subirlos a producción para asegurar que

la imagen base no tiene fallos críticos conocidos.
- Corrección preventiva: Identificación de inyecciones SQL o fallos de lógica de negocio mientras el programador escribe código en VS Code.

Uso y distribución
- Versión web: Panel de control centralizado y analítica.
- Extensiones del navegador y plugins IDE: VS Code, JetBrains (IntelliJ, PyCharm), Eclipse y Visual Studio.
- Versión escritorio: Integración nativa con sistemas operativos vía CLI.
- CLI: Herramienta de línea de comandos potente para automatizaciones locales y scripts.

Open source
Snyk ofrece tests ilimitados y gratuitos para repositorios públicos, posicionándose como una herramienta estándar para mantenedores de código abierto.

Integraciones
- Facilidad de integración: Alta (Low-code mediante integraciones nativas).
- API propia: Dispone de REST API completa (principalmente en planes Enterprise) para extraer datos de vulnerabilidades hacia BI o herramientas propias.
- Almacenamiento y Repositorios: GitHub, GitLab, Bitbucket (Cloud y Server), Azure Repos.
- CI/CD: Jenkins, CircleCI, GitHub Actions, AWS CodePipeline.
- Registro de contenedores: Docker Hub, Amazon ECR, JFrog Artifactory.

Notas finales
Información legal, licencias y contratos
- Propiedad Intelectual: El código analizado no es propiedad de Snyk; la herramienta procesa metadatos pero el cliente mantiene la titularidad total.
- Cumplimiento: Certificaciones SOC 2 Tipo II, cumplimiento de RGPD e ISO 27001.

Para más información:
- Sitio web oficial: https://snyk.io
- Precios: https://snyk.io/pricing
- Documentación técnica: https://docs.snyk.io
- Términos de servicio: https://www.snyk.io/policies/terms-of-service/
- Github oficial: https://github.com/snyk

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Snyk es una plataforma de seguridad **"developer-first"** diseñada para integrar la detección y corrección de vulnerabilidades directamente en el flujo de trabajo de desarrollo (SDLC). Es ideal para empresas que operan bajo metodologías **Agile y DevOps**, permitiendo que la seguridad no sea un cuello de botella.
- **Tipos de empresa:** Desde pequeñas startups tecnológicas hasta grandes corporaciones (Banca, Seguros, Telco) que gestionan infraestructuras críticas o datos sensibles.
- **Puntos clave:** Automatización de la remediación (Fix PRs), escaneo de dependencias (SCA), código propio (SAST), contenedores y plataformas de infraestructura como código (IaC).

Madurez digital requerida
- **Usuarios/Equipo:** Nivel medio-alto. Los desarrolladores deben estar familiarizados con el uso de **Git y entornos de CI/CD** (Jenkins, GitHub Actions, GitLab CI). Es necesario que el equipo entienda conceptos básicos de vulnerabilidades (CVE) y severidad.
- **Empresa/Departamentos:** Requiere una cultura de **responsabilidad compartida** entre Seguridad y Desarrollo. La empresa debe haber superado la fase de revisiones manuales aisladas y estar en proceso de automatización de sus pipelines de despliegue.

Plan orientativo de implantación
Pasos necesarios y estimaciones
El despliegue completo en una organización media puede oscilar entre **2 y 6 meses**, dependiendo del número de repositorios y la complejidad de las políticas.
- **Fase 1: Discovery (1-2 semanas):** Identificación de aplicaciones críticas, lenguajes de programación y herramientas de CI/CD actuales. Definición de administradores de grupo.
- **Fase 2: Piloto (2-4 semanas):** Selección de un equipo "influencer" para integrar Snyk en sus repositorios. Configuración de los primeros escaneos en IDEs y Pull Requests para ajustar el ruido (falsos positivos).
- **Fase 3: Configuración de Políticas (2 semanas):** Establecimiento de reglas de cumplimiento (ej. bloquear builds si hay vulnerabilidades críticas o licencias legales no permitidas).
- **Fase 4: Despliegue Masivo (1-3 meses):** Integración progresiva en el resto de departamentos y configuración de Single Sign-On (SSO) en planes Enterprise.
- **Fase 5: Seguimiento y Feedback:** Revisión trimestral de KPIs de seguridad y ajuste de gobernanza.

Necesidades de formación del equipo
- **Talleres técnicos:** Sesiones prácticas sobre cómo interpretar los informes de Snyk y cómo aplicar los "Auto-fix PRs".
- **Canales internos:** Creación de comunidades de práctica (Slack/Teams) para resolver dudas sobre triaje de vulnerabilidades.
- **Documentación propia:** Adaptación de las guías de Snyk a los estándares específicos de codificación de la empresa.

Perfiles necesarios
- **Líder de Seguridad de Aplicaciones (AppSec):** Define las políticas y supervisa el cumplimiento global.
- **Ingeniero DevOps:** Se encarga de la integración técnica en los pipelines de CI/CD y gestión de APIs.
- **Developer Champions:** Desarrolladores dentro de cada equipo que actúan como referentes en el uso de la herramienta.

Retorno de la inversión (ROI)
- **Productividad:** Reducción del **60% en el tiempo de remediación** y hasta un 75% si la vulnerabilidad se detecta en el IDE antes de llegar al repositorio.
- **Ahorro de costes:** Según estudios de Forrester, las organizaciones pueden alcanzar un **ROI del 288% en 3 años**, recuperando la inversión inicial en menos de 6 meses.
- **KPIs principales:** Tiempo Medio de Remediación (MTTR), número de vulnerabilidades críticas en producción y porcentaje de proyectos con cobertura de escaneo activa.

Otros
- **Barrera de precio:** Existe un salto significativo de coste al pasar de 10 desarrolladores (Plan Team) a planes Enterprise, lo cual debe ser previsto en presupuestos anuales.

- **Mantenimiento:** Requiere reservar unas 2-4 horas mensuales para mantenimiento de integraciones y actualización de configuraciones de CLI.

PREGUNTAS FRECUENTES

¿Qué es Snyk y cuál es su enfoque principal?
Snyk es una plataforma de seguridad orientada al desarrollador (developer-first) que se integra en el ciclo de vida de desarrollo de software (SDLC). Su objetivo es identificar y corregir vulnerabilidades en el código, dependencias de código abierto, contenedores e infraestructura como código de manera automatizada.

¿Para qué sirve exactamente esta herramienta en un entorno profesional?
Sirve para mitigar riesgos de seguridad sin detener la velocidad de entrega. Permite automatizar el análisis estático de código (SAST), la gestión de dependencias (SCA), el escaneo de imágenes de contenedor y la validación de configuraciones de infraestructura (IaC), proporcionando soluciones directas como Pull Requests automáticos.

¿Qué coste tiene el servicio para empresas y profesionales?
Snyk ofrece una versión gratuita para desarrolladores individuales con límites mensuales de escaneo. El plan 'Team' tiene un coste aproximado de 25€ al mes por desarrollador, mientras que el plan 'Enterprise' requiere presupuesto personalizado. Existe también un plan 'Ignite' para medianas empresas por unos 1.260€ anuales por desarrollador.

¿Existe una versión gratuita o para proyectos Open Source?
Sí, la plataforma ofrece tests ilimitados y gratuitos para repositorios públicos de código abierto. Para proyectos privados, la versión gratuita incluye hasta 200 análisis de código abierto, 100 de contenedores y 300 de infraestructura como código al mes.

¿Es Snyk una herramienta de código abierto (Open Source)?
No, Snyk es una plataforma comercial propietaria (SaaS). Sin embargo, es ampliamente utilizada en la comunidad Open Source y ofrece herramientas de línea de comandos (CLI) cuyo código es accesible y contribuible a través de su cuenta oficial de GitHub.

¿Cumple con la normativa española y europea de protección de datos?
Sí, Snyk cumple con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Además, cuenta con certificaciones internacionales de seguridad como SOC 2 Tipo II e ISO 27001, garantizando estándares elevados de cumplimiento legal y técnico.

¿Cómo garantiza la privacidad del código analizado?
La plataforma procesa metadatos y firmas de código para detectar vulnerabilidades, pero la propiedad intelectual del código analizado permanece íntegramente bajo la titularidad del cliente. Snyk implementa medidas de aislamiento de datos y cifrado para asegurar que la información sensible no sea expuesta.

¿Es una tecnología segura para integrar en infraestructuras críticas?
Se considera una tecnología segura y robusta, validada por empresas del IBEX 35 y corporaciones tecnológicas globales. Su base de datos de vulnerabilidades propia suele actualizarse con mayor rapidez que la base de datos nacional de vulnerabilidades (NVD), permitiendo una respuesta más ágil ante amenazas de día cero.

¿Con qué herramientas y entornos de desarrollo se puede integrar?
Se integra de forma nativa con los principales IDE (VS Code, IntelliJ, Eclipse, Visual Studio), sistemas de control de versiones (GitHub, GitLab, Bitbucket), plataformas de CI/CD (Jenkins, GitHub Actions, CircleCI) y registros de contenedores como Docker Hub o Amazon ECR.

¿Qué nivel técnico se requiere para implementar Snyk?
Para el uso diario el nivel es medio, ya que el desarrollador solo debe interpretar las alertas. No obstante, para la instalación y configuración inicial se requiere un perfil medio-alto con conocimientos en pipelines de CI/CD, gestión de repositorios Git y administración de infraestructura o sistemas DevOps.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- Realizar una Evaluación de Impacto de Protección de Datos (EIPD) antes de la integración, especialmente si se vinculan repositorios que contienen datos de carácter personal o configuraciones críticas de infraestructura.
- Configurar el control de acceso basado en roles (RBAC) para limitar quién puede visualizar las vulnerabilidades detectadas, evitando la exposición de debilidades del sistema a personal no autorizado.
- Revisar específicamente la política de retención de datos en la consola de Snyk para asegurar que los informes de escaneo se eliminan cuando dejan de ser necesarios para la operativa.
- En caso de utilizar Snyk Code (IA), verificar en la configuración que los fragmentos de código enviados para análisis no se utilicen para el reentrenamiento de modelos globales de la plataforma, protegiendo así el secreto comercial y la propiedad intelectual.
- Firmar el Acuerdo de Procesamiento de Datos (DPA) estándar de la entidad para formalizar la relación de encargado de tratamiento según el RGPD.

Ley de Inteligencia Artificial (AI Act)
- Clasificación de riesgo: Snyk utiliza sistemas de IA (Snyk Code) para el análisis estático de seguridad (SAST). Bajo la Ley de IA de la UE, estas herramientas se consideran generalmente de riesgo limitado o bajo, al ser herramientas de soporte técnico para profesionales.
- Transparencia: La herramienta debe informar claramente cuando los resultados (sugerencias de código o correcciones) son generados por modelos de IA.
- Control humano: Las "pull requests" automáticas generadas por la IA no deben ejecutarse sin la supervisión y validación de un desarrollador humano responsable del impacto del cambio.

Privacidad y protección de datos
- Responsabilidades: La empresa española actúa como Responsable del Tratamiento y Snyk (Snyk Limited/Inc) actúa como Encargado del Tratamiento.
- Ubicación de los datos: Snyk ofrece opciones de residencia de datos (Data Residency) principalmente para clientes Enterprise, permitiendo el alojamiento en regiones de la UE (como Frankfurt). En planes inferiores, los datos pueden ser procesados en ubicaciones globales.
- Transferencia internacional: Existe transferencia de datos fuera del Espacio Económico Europeo (EE. UU.). Esta se fundamenta en las Cláusulas Contractuales Tipo (SCCs) incluidas en su DPA y en su certificación bajo el Marco de Privacidad de Datos EU-EE. UU. (Data Privacy Framework).
- Derechos ARCO: La empresa debe garantizar que puede gestionar las solicitudes de acceso, rectificación o supresión de los desarrolladores cuyos datos (nombres de usuario, correos electrónicos en logs de commit) son procesados por la plataforma.

Propiedad intelectual
- Propiedad de datos: El cliente mantiene todos los derechos de propiedad técnica sobre el código fuente, archivos de configuración y manifiestos escaneados. Snyk no adquiere derechos de propiedad sobre los activos del cliente.
- Propiedad del resultado/procesamiento/propiedad intelectual: Los informes de vulnerabilidad generados son propiedad de la empresa cliente. Snyk conserva la propiedad intelectual de sus algoritmos de detección, su base de datos de vulnerabilidades (Snyk Intel DB) y su motor de IA.
- Gestión de licencias: Snyk permite auditar licencias de terceros (como GPL, MIT, Apache) para asegurar que el software desarrollado por la empresa cumple con las obligaciones de propiedad intelectual de sus dependencias y evitar el "efecto contagio" de licencias copyleft en productos comerciales.

Usos y prohibiciones
- Usos prohibidos: No se permite el uso de la plataforma para realizar ingeniería inversa de los servicios de Snyk, el uso de la API para extraer masivamente la base de datos de vulnerabilidades con fines comerciales ajenos, o el uso de la herramienta para actividades de hacking malicioso.
- Usos admitidos: Uso profesional para la detección de errores de seguridad, gestión de cumplimiento de licencias de software y aseguramiento de la cadena de suministro de software (Software Supply Chain).

Seguridad y certificaciones
- Seguridad: Cifrado de datos en tránsito (TLS 1.2+) y en reposo (AES-256). Snyk procesa metadatos tras el escaneo inicial para minimizar la exposición del código fuente completo.

- Certificaciones: Dispone de SOC 2 Tipo II e ISO 27001, lo que garantiza estándares internacionales de gestión de la seguridad de la información.

Otros
- Responsabilidad Profesional: El uso de Snyk no exime a la empresa de su responsabilidad legal en caso de una brecha de seguridad. La herramienta es un medio de prevención, no una garantía de inmunidad legal ante el RGPD.

Fuentes consultada:
- Contratos: https://snyk.io/policies/terms-of-service/
- Certificaciones: https://snyk.io/platform/security-and-compliance/
- Condiciones: https://snyk.io/policies/dpa/
- Licencias: https://github.com/snyk/snyk/blob/master/LICENSE