SECURE EVERY LAYER, EMPOWER EVERY TEAM:

The Unified Snyk Platform

snyk

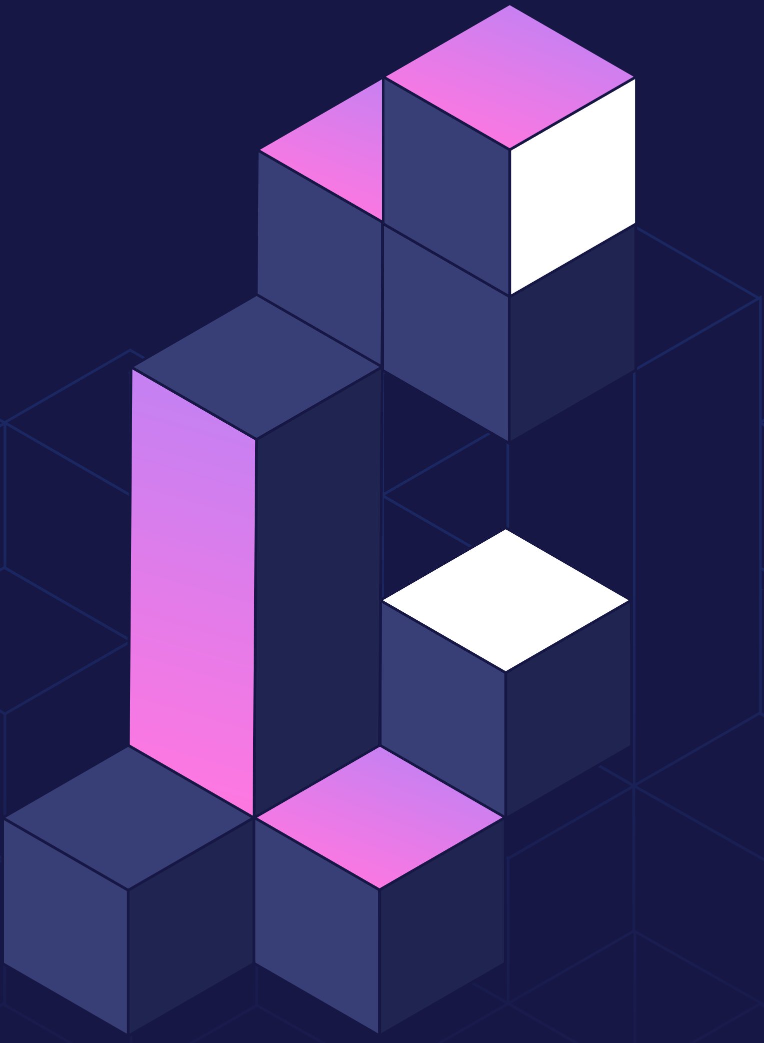
DEVELOPER SECURITY FOR THE AI ERA

Application security has never been more tightly woven into the fabric of how software is built. Integration into developer workflows, once a forward-looking goal of DevSecOps, is now a baseline expectation.

However, with the rise of generative AI tools accelerating development and producing more code than ever, the scale and speed of software creation have grown exponentially. As organizations embrace cloud-native architectures, scale development across globally distributed teams, and adopt AI to boost velocity, one truth becomes even clearer: security must meet developers exactly where they are inside the tools, workflows, and pipelines they use every day and it must do so with automation and intelligence capable of keeping up with both humans and machines.

Today's application security challenges are inseparable from three converging forces: how developers work, the surge in AI adoption, and the growing demand for unified platforms that eliminate friction between security and engineering teams. Developers move fast, AI accelerates complexity, and tool sprawl creates gaps in coverage. What teams need isn't just more security. They need smarter, more integrated security that works with them, not against them.

That's exactly what Snyk was built to do. As an AI trust platform that puts developers first, Snyk enables secure software delivery from code to the cloud, embedding security at every step of the development lifecycle. It unifies critical security functions across proprietary code, open source dependencies, containers, infrastructure as code, and APIs. And it does so with AI-enhanced automation that scales visibility, accelerates remediation, and enables engineering teams to stay focused and productive.



The Snyk AI Trust Platform supports this evolution as an intelligent foundation that brings consistency, context, and trust to the way security automation is applied. It powers key workflows like **Snyk Assist, Snyk Agent Fix**, and **Snyk Studio** behind the scenes, ensuring that AI delivers value without sacrificing control or introducing risk. It's a future-ready layer designed to grow with your team's needs, not dictate them.

Underpinning future development, Snyk Labs is an internal research and experimentation hub focused on emerging AI security risks. Current areas of investigation fall under the umbrella of AI Security Posture Management (AI-SPM) and include initiatives like AI bill of materials (AI-BOM) analysis, model risk registries, threat modeling, and red teaming techniques to address risks such as model jailbreaking. Insights from Snyk Labs are intended to shape future platform capabilities and contribute to developing broader AI security standards across the industry.

In parallel, Invariant Labs is exploring new frontiers in agent security, researching how to secure AI agents and their interactions within complex environments. This is a critical area as organizations begin to operationalize AI more deeply.

Finally, Snyk Studio extends the AI Trust Platform through partner collaboration, providing a dedicated environment for technology vendors to integrate Snyk's security capabilities into AI-assisted development tools. At the core is the Snyk MCP Server, a standardized interface that enables third-party AI models (e.g., coding assistants and agentic platforms) to incorporate Snyk's security intelligence and policy logic. This allows developers to access real-time guidance and enforce guardrails directly within AI-driven workflows.

We'll break down what makes the Snyk platform unique:

- A look at the **core engines** securing every layer of the application stack
- The **platform add-ons** that expand visibility, risk context, and developer education
- The **AI-powered workflows** that make security more accessible and actionable
- A real-world example of how these pieces come together inside a modern organization
- And tailored insights into how Snyk delivers value to developers, security teams, and engineering leaders alike

Let's look closer at how Snyk helps teams build fast and fix faster with confidence by reducing risk in software development, enabling faster innovation, and helping teams efficiently deliver secure software.

THE SNYK PLATFORM AT A GLANCE

The Snyk AI Trust Platform delivers unified, developer-first security and AI trust across every layer of modern application development, from code to cloud, through a single, integrated system. It enables seamless collaboration between development and security teams to build faster, securely, and at scale.

At the heart of the platform are intelligent engines that secure proprietary code, open-source dependencies, containers, infrastructure as code (IaC), and APIs. These engines are embedded directly into developer workflows, enabling in-flow issue detection and guided remediation from the IDE to your CI/CD pipeline. The platform ensures faster, smarter security without disrupting the way developers work. It is powered by AI-driven capabilities like **Snyk Assist, Snyk Agent Fix,** and **Snyk Studio + Labs.**

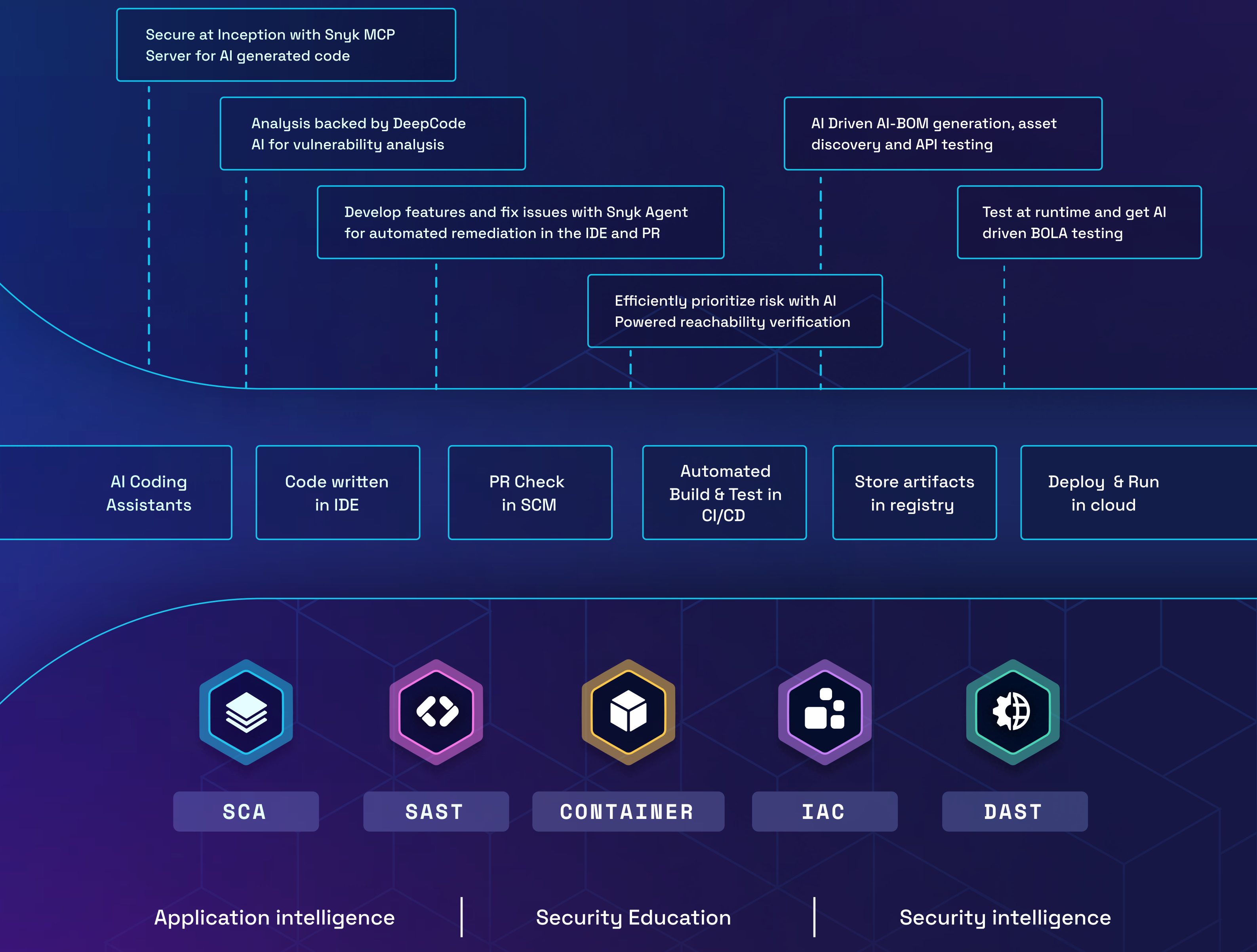
Surrounding these capabilities is a cohesive layer of collaboration, visibility, and governance. Platform add-ons like Snyk Learn and Snyk Analytics provide integrated education and actionable reporting to help dev, sec, and platform teams work together toward a common security goal. Unified analytics and centralized administration simplify onboarding, integration, and scaling across teams and tools.

With enterprise-grade coverage, intelligent automation, and seamless developer experience, the Snyk AI Trust Platform brings consistency, speed, and trust to modern software delivery. Designed to provide teams with the tools they need in the context they want, the platform empowers you to scale your secure development practice.

THE RESULTS

- **Developer Experience:** Embedded across the SDLC, enabling developers to secure as they build without disrupting flow
- **Depth of Testing:** High-accuracy analysis using SAST, SCA, DAST, container, and IaC engines
- **Intelligent Insights:** AI-powered context to prioritize risk and drive faster fixes

SNYK:AI-ACCELERATED DEVSECOPS ACROSS THE SDLC



Secure at Inception with Snyk MCP Server for AI generated code

Analysis backed by DeepCode AI for vulnerability analysis

Develop features and fix issues with Snyk Agent for automated remediation in the IDE and PR

Efficiently prioritize risk with AI Powered reachability verification

AI Driven AI-BOM generation, asset discovery and API testing

Test at runtime and get AI driven BOLA testing

AI Coding Assistants

Code written in IDE

PR Check in SCM

Automated Build & Test in CI/CD

Store artifacts in registry

Deploy & Run in cloud

SCA

SAST

CONTAINER

IAC

DAST

Application intelligence | Security Education | Security intelligence

Snyk core engines — secure every layer

Snyk's core products form the foundation of its developer-first platform, each focused on securing a critical layer of the modern application stack. Unified by common workflows and integrated directly into developer tools, they work together to surface issues early, enable fast fixes, and reduce risk at scale. The following sections will explore how these engines power secure development from code to cloud and how, when combined, the whole platform goes beyond shifting security left and DevSecOps, providing a path to embracing AI without introducing risks.

SNYK CODE

Snyk Code is where secure development begins. Focused on proprietary code, it identifies vulnerabilities like injection flaws, insecure deserialization, and improper data handling issues that, if left unchecked, can introduce serious risks deep within an application's foundation.

It integrates directly into popular IDEs and Git platforms, delivering real-time feedback as developers write, review, and commit code. Security findings are presented in context, with clear fix suggestions that make it easier to resolve issues without disrupting momentum.

What sets Snyk Code apart isn't just how naturally it fits into the developer workflow. The speed, accuracy, and actionability of its results, powered by an AI-driven engine, surface issues in real-time without requiring a build. That means developers instantly get meaningful insights without adding extra steps to their pipeline.

Snyk Code helps teams catch problems early and often. When paired with **Snyk Agent Fix**, it enables in-flow remediation at both the IDE and PR stages, helping developers go from detection to secure resolution in a matter of clicks.

SNYK OPEN SOURCE

Modern applications rely heavily on open source, but with that speed and flexibility comes risk. Snyk Open Source helps teams manage hidden vulnerabilities, outdated dependencies, and license risks that can lurk within third-party packages across ecosystems like npm, Maven, and PyPI; risks that directly impact the software supply chain.

By scanning manifest and lock files directly within IDEs, repositories, and CI pipelines, Snyk Open Source delivers continuous visibility into the state of your dependencies. When issues are found, it goes beyond flagging them. It prioritizes what to fix first with reachability analysis and offers clear upgrade paths, including automated pull requests to accelerate remediation.

It also supports SBOM generation and monitoring, helping teams track component usage and comply with software supply chain requirements.

Snyk Open Source is backed by the Snyk Vulnerability Database, a comprehensive, research-driven resource maintained by Snyk's security team. Updated faster than competing databases and enriched with human-curated insights, it enables earlier detection and more actionable fixes. With over 3x the coverage of the next largest commercial database, it gives teams the intelligence advantage they need to stay ahead.

Integrated deeply into the Snyk platform, Snyk Open Source reduces exposure before code ever reaches production and feeds rich vulnerability data to **Snyk Analytics**, offering a broader view of application risk across projects and teams.

SNYK CONTAINER

As container adoption continues to accelerate, so do the security challenges that come with it. Snyk Container is purpose-built to help teams secure their containerized applications by identifying known vulnerabilities in container images and base OS layers and misconfigurations that could pose risks at runtime.

It integrates seamlessly with Docker, Kubernetes, and major container registries, embedding directly into CI/CD pipelines to provide in-context scanning during build, deployment, and image push. With detailed base image intelligence and upgrade recommendations, Snyk Container helps teams make informed decisions before vulnerable images reach production.

Snyk Container plays a key role in the broader platform by extending application security visibility into container environments. It works hand-in-hand with **Snyk IaC** to support governance and enforcement across cloud-native infrastructure.

Snyk Open Source goes beyond flagging issues, it prioritizes what to fix first with reachability analysis and offers clear upgrade paths, including automated pull requests to accelerate remediation.

SNYK INFRASTRUCTURE AS CODE (IAC)

Misconfigurations in cloud infrastructure can expose critical systems before a single workload is deployed. Snyk IaC helps teams catch these issues early by scanning infrastructure as code templates, including Terraform, Kubernetes, and CloudFormation, for security and compliance risks like open ports, excessive permissions, and non-compliant resource definitions. It surfaces policy violations as developers write infrastructure code directly in the IDE, repositories, and CI/CD pipelines, and provides clear fix suggestions and inline guidance.

Snyk IaC supports end-to-end governance when used alongside **Snyk Container**, helping teams secure their infrastructure from code to runtime.

PLATFORM ADVANTAGE: WHEN EVERYTHING WORKS TOGETHER

Each of the engines powering the Snyk Platform provides developer-first, easy-to-use solutions, best-in-class accuracy, and the speed at scale required to accelerate innovation while delivering secure software. The value of the core elements compounds, providing your teams with a powerful system for application security governance that protects and enables organizations to develop fast and stay secure. Extend the best platform further with add-ons.

SNYK API & WEB

APIs and web applications are the backbone of modern software and some of the most exposed parts of the attack surface. Snyk API & Web helps secure these critical components by detecting runtime risks and vulnerabilities across integration points, automation workflows, and externally exposed services.

It integrates through powerful APIs and webhook support, making it easy to embed security into CI/CD pipelines and cloud-native environments. With accurate detection and a false positive rate of just 0.08%, Snyk API & Web helps teams focus on what truly matters. Automated scanning, policy enforcement, and scalable reporting ensure they stay ahead of threats without slowing delivery.

By extending security testing beyond commit to include running applications in staging or production-like environments, **Snyk API & Web** expands the platform's ability to detect real-world, runtime-accessible vulnerabilities.

Snyk API & Web expands the platform's ability to detect real-world, runtime-accessible vulnerabilities.

Platform add-ons — scale visibility and skills

While Snyk's core testing engines secure every layer of the application stack, the platform add-ons elevate that foundation by providing the visibility, context, and guidance needed to scale security across teams and environments. These capabilities help organizations move beyond simply identifying issues. They empower teams to understand, prioritize, and respond to risk in smarter, faster ways. In the next section, we'll explore how these add-ons extend the value of the Snyk platform and support organizations as they grow their security maturity.

SNYK ESSENTIALS

Snyk Essentials gives organizations a fast, structured path to operationalizing application security at scale. Designed for teams building or expanding developer-first security practices, it goes beyond scanning to provide the context and control needed to manage risk effectively from day one.

At its core, Essentials automatically discovers and continuously maps the full application surface, pulling in repositories, packages, container images, and more from your existing toolchains. It enables your teams to build policies that automate tagging, classification, and actions based on asset attributes or risk profiles so that governance keeps pace with growth. Define and enforce scanning requirements across code, open source, containers, and IaC. Once assets are identified and policies are defined, Snyk Essentials ensures critical projects are tested according to business and compliance standards without relying on manual oversight.

To help teams focus capacity on what truly matters, Snyk Essentials adds application and business context to the technical vulnerability insights that Snyk's testing engines provide. By factoring in asset importance, business impact, and exposure, Essentials enables more efficient, risk-based prioritization, helping development and security teams align quickly on the highest-value remediation work without getting buried in noise.

Snyk Essentials simplifies the platform rollout, tightens feedback loops, and builds confidence in every security decision, helping teams move faster while staying secure.

SNYK LEARN

Security education is too often treated as a checkbox exercise delivered once a year through outdated, generic training platforms that bear little relevance to a developer's actual work. It's time-consuming, disconnected, and rarely helpful at the moment it's needed most. Snyk Learn flips that model, delivering contextual, just-in-time lessons exactly when a developer encounters an issue right inside their IDE, CLI, or pull request.

Instead of sitting through irrelevant modules, developers learn through targeted training aligned with the specific vulnerability they're addressing. If a cross-site scripting (XSS) issue is found, they get a focused lesson on XSS, no searching, no guesswork. Lessons cover modern security topics like the **OWASP Top 10, secure AI adoption,** LLM-related risks, and product-specific queries tied directly to Snyk findings.

The **Snyk Learning Management Add-On** further elevates the experience, enabling organizations to assign learning paths, track developer progress, and generate audit-ready reports for compliance with PCI DSS, SOC 2, SOX, ISO 27001, and more.

Within Snyk Learn, **Snyk Assist** provides access to an AI-powered mentor for real-time support and clarification, reinforcing learning and boosting confidence without interrupting the flow. Together, Snyk Learn and the Learning Management Add-On strengthen security culture, meet compliance needs, and help teams scale developer enablement in a way that's finally built for how modern software gets built.

SNYK ANALYTICS

Security can't be improved if it can't be measured. Snyk Analytics gives teams the clarity they need to understand their security posture, track progress, and communicate impact, all from a single, unified view. With dashboards that surface everything from vulnerability trends and fix velocity to policy adherence and tool adoption, it turns raw security data into meaningful, actionable insight.

By pulling real-time telemetry across all Snyk engines and AI-powered workflows, Snyk Analytics supports detailed reporting at the team and executive level. Whether it's a developer tracking open issues or a security leader preparing for a quarterly business review, customizable filters, and export-ready views make it easy to share progress and identify where to focus next.

Snyk Analytics powers data-driven conversations between engineering, AppSec, and leadership in the broader platform. It helps demonstrate the impact of developer-first security initiatives, supports compliance and reporting requirements, and enables continuous improvement by revealing gaps in coverage, adoption, or remediation activity before they become systemic.

> Snyk Assist provides access to an AI-powered mentor for real-time support and clarification, reinforcing learning and boosting confidence without interrupting the flow.

AI workflows — intelligence across the SDLC

With security teams stretched thin and development moving faster than ever, automation isn't just helpful, but a core component for success. That's where Snyk's AI-powered workflows come in. Built to amplify human effort, these tools bring intelligent guidance, trusted remediation, and adaptive policy enforcement into the development lifecycle. In the following section, we'll explore how Snyk uses AI not to replace developers and security teams but to help them move faster, fix smarter, and scale security with confidence.

SNYK ASSIST

Snyk Assist brings intelligent, in-the-moment support to the developer experience. Acting as a real-time AI assistant, it delivers contextual guidance precisely when it's needed, helping developers understand vulnerabilities, explore secure alternatives, and move forward with confidence, all without breaking flow.

Tightly integrated with Snyk Learn, Snyk Assist turns every security finding into a learning opportunity by explaining what needs to be fixed and why it matters. It reduces friction, removes ambiguity, and accelerates secure decision-making where it matters most inside the development workflow.

For developers, it means faster clarity and fewer roadblocks. For AppSec teams, it's a scalable way to embed security expertise into every line of code with no extra tickets and no delays.

SNYK AGENT FIX

Snyk Agent Fix takes security automation a step further by fixing the issues identified by testing engines. It acts as a trusted partner in the development process, integrating into the developer's workflow to automatically generate and validate safe, production-ready fixes directly within the IDE and pull requests.

Snyk Agent Fix removes the guesswork and manual overhead from vulnerability resolution by applying learned remediation patterns. Thanks to patented CodeReduce tech and pre-validated fixes, it is industry-leadingly accurate at 80%, giving developers the confidence to move quickly without compromising code quality or introducing regressions.

For engineering teams working at scale, Snyk Agent Fix delivers a powerful advantage: low-friction, high-impact security that keeps pace with rapid development cycles and integrates remediation seamlessly into CI/CD workflows.

SNYK STUDIO

Snyk Studio opens the door for deeper innovation and customization by giving partners and advanced users a collaborative space to extend the platform. Designed for those building at the edge of AI and automation, Studio enables seamless integration of Snyk testing into third-party tools, developer agents, and GenAI platforms.

With capabilities like private API access and the Snyk MCP Server, ecosystem partners can embed secure development practices directly into AI-powered workflows. **Snyk Studio** isn't just an integration layer. It's a launchpad for experimentation, supported by Snyk Labs, where forward-looking ideas and early-stage tools take shape.

For platform engineers, security teams, and AI innovators, Snyk Studio provides the flexibility to tailor security to their environment, helping them move faster, test smarter, and stay ahead of what's next. It enables security at inception by securing the code generated by AI, as it's generated by AI.

> Snyk Agent Fix acts as a trusted partner in the development process, integrating into the developer's workflow to automatically generate and validate safe, production-ready fixes directly within the IDE and pull requests. It is industry-leadingly accurate at 80%, giving developers the confidence to move quickly without compromising code quality or introducing regressions.

Platform in action — Empowering developers and security teams

Seeing the Snyk platform in motion helps you understand the real impact. Imagine a typical day inside a fast-moving development team. A developer starts by writing code in their IDE with an AI copilot. As they code, Snyk Code scans along in real-time. If a security issue pops up, the developer is able to immediately apply a validated fix for the issue generated by Snyk Agent Fix. Rather than filing a ticket or pinging security, they address it on the spot and keep moving.

At the next desk over, the developer's counterpart is working on another application component. The AI tool this dev uses generates code for a new feature, including a new, insecure open-source library in the app. Snyk Open Source identifies the new dependency as insecure and reachable, and offers a quick fix before the code is committed and merged to the main branch.

As the code moves through CI/CD, Snyk continues applying security controls, scanning for issues, enforcing policies, and integrating seamlessly into the release pipeline. When deciding what to fix first, Snyk's Risk-Based Prioritization helps teams focus on what matters most. Powered by the Snyk Risk Score, this model combines multiple layers of context from technical factors like EPSS and static reachability, to application-level insights and business impact to guide security and development teams toward the highest-value remediation work.

The security team recognizes that a business-critical application has slipped through the cracks and is not being tested by Snyk API & Web. In order to remain compliant with industry-relevant regulations, the app must be tested dynamically at runtime to ensure customer data is protected. The team quickly grabs the latest production-ready build, easily tests it with Snyk API & Web to identify security issues introduced in API connections or at runtime, and is relieved to find no issues!

Later, as the security team does a programmatic review of the secure software development practice they've built, they check **Snyk Analytics** to monitor fix velocity, policy compliance, and overall platform adoption. The trend is clear, developers are adopting more Snyk testing, identifying issues earlier in the development lifecycle, and fixing them faster, efficiently delivering secure software. Executive reporting is just a few clicks away. From there, policy-driven automation ensures the team isn't just reacting. They're continuing to iterate on the scaled DevSecOps program they've built, implementing smarter processes that proactively prevent recurring issues and support further scale.

This continuous cycle of detection, prioritization, remediation, and governance all flows through the Snyk platform, helping teams move faster, stay secure, and make smarter decisions at every stage.

Why Snyk? Tailored value for each role

The strength of the Snyk platform isn't just in its features. It's in how well it adapts to the needs of the people using it. From hands-on developers to security teams and platform engineers, Snyk delivers targeted value that aligns with each role's priorities. The platform helps every stakeholder move faster, work smarter, and contribute to building secure software at scale.

DEVELOPERS

Security works best when it supports development, not when it disrupts it. That's why Snyk is built for developers, helping them stay in flow, fix issues faster, and ship secure code without added friction. Instead of introducing more tools or creating extra steps, Snyk brings security directly into developers' environments.

Real-time guidance appears right in the IDE, offering immediate feedback on issues as code is written, no jumping between tools, and no delays. When problems arise, Snyk provides clear, actionable fixes that make remediation intuitive, whether suggesting a safer dependency or flagging a risky configuration.

AI-powered tools like **Snyk Assist** and **Snyk Agent Fix** give developers the confidence to commit, offering intelligent recommendations and auto-validated fixes before code is merged. Meanwhile, **Snyk Learn** delivers just-in-time lessons tied to actual issues, helping developers build security knowledge as they work.

And because Snyk integrates across the entire toolchain from IDE to Git repos, CI/CD to CLI, developers can focus on building, not battling security blockers.

SECURITY TEAMS

Balancing risk reduction with development speed has always been challenging for security teams. Snyk bridges that gap by putting powerful security capabilities directly into the hands of developers without giving up control or visibility. With Snyk, security teams can move from gatekeeping to guiding, helping accelerate delivery while strengthening defenses.

By embedding security into developer tools and workflows, Snyk enables faster remediation of issues further left in the development lifecycle, shortening the vulnerability lifecycle. Teams can codify and automate policies that apply consistently across the stack, from code and dependencies to containers and infrastructure as code, ensuring enforcement at scale without constant manual oversight.

Snyk Analytics provide unified visibility across the organization, eliminating silos and making it easier to track progress, coverage, and compliance. Security teams can shift left without slowing anyone down because Snyk integrates where developers work in the IDE, PR, and pipeline. With audit-ready oversight and scalable governance, Snyk helps security teams do more than keep up. It helps them lead.

PLATFORM TEAMS

For platform teams, Snyk simplifies one of the hardest challenges: consolidating fragmented tools and embedding security without disrupting developer workflows. By unifying SAST, SCA, container, IaC, and DAST capabilities into a single platform, Snyk helps reduce tool sprawl and streamline secure development across the entire SDLC.

With Snyk Analytics, platform teams can monitor adoption, fix rates, and vulnerability trends, ensuring developers engage with security in meaningful, trackable ways.

Snyk integrates cleanly into existing pipelines and tooling, reducing friction for developers and minimizing overhead for platform teams. It supports consistent policy enforcement, helps ensure audit and compliance readiness, and makes it easier to scale security practices across diverse teams and environments.

As internal demand for AI tools grows, Snyk provides the controls platform teams need to govern usage and maintain oversight, enabling innovation without sacrificing alignment or accountability.

> The strength of the Snyk platform isn’t just in its features. It’s in how well it adapts to the needs of everyone using it. From hands-on developers to security teams and platform engineers, Snyk delivers value that aligns with priorities. The platform helps every stakeholder move faster, work smarter, and contribute to building secure software at scale.

LET'S GET TO WORK

Software moves fast, and security needs to move with it. That's precisely what the Snyk platform is built for. From the first line of code to live production environments, Snyk gives your team the tools to build securely without breaking stride. It's not about adding more steps. It's about removing blockers and turning security into a natural part of how great software gets made.

Throughout this guide, you've seen how Snyk integrates into the way modern teams actually work. Developers get real-time feedback and in-flow fixes. Security teams gain visibility and control without bottlenecks. Leaders get clarity, accountability, and momentum. This isn't a theory. It's what secure development looks like when everything clicks.

Ready to make it real? Book a demo to see the Snyk AI Trust Platform in action.

snyk