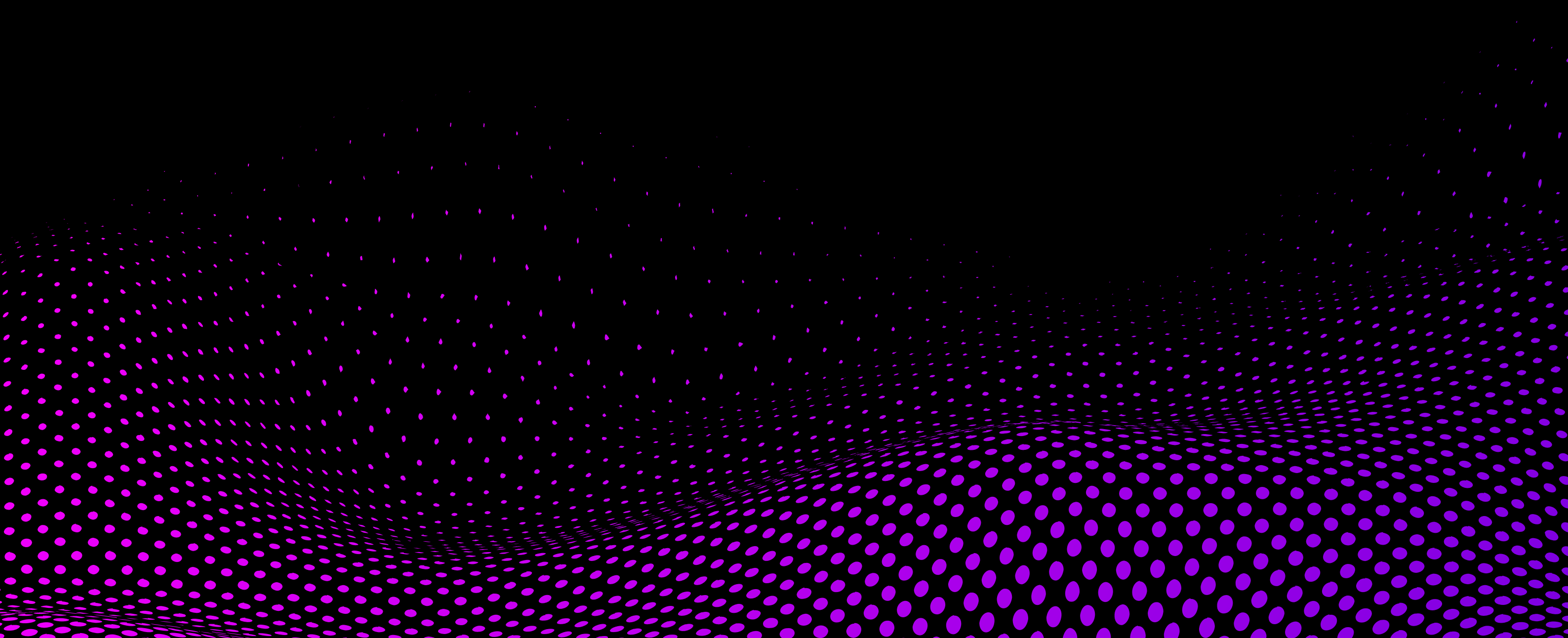
WHITE PAPER

Securing AI at Scale

Operationalizing the AI Security Fabric with Snyk



Securing software in the AI era

The rise of Artificial Intelligence (AI) has shattered traditional security paradigms, introducing a crisis of non-deterministic security chaos. As humans, models, and autonomous agents generate code at machine speed, a widening gap has emerged between builder velocity and security governance. Legacy application security tools, built for a rule-based, deterministic past, are unable to keep pace with this new velocity or manage the blind spots created by the AI software supply chain. It has never been so important to weave application security into the fabric of how software is built. Integration into developer workflows, once a forward-looking goal of DevSecOps, is now a baseline requirement.

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.

To bridge this gap, Snyk is weaving the **AI Security Fabric**: an invisible, intelligent layer that provides continuous, autonomous defense across the entire software development lifecycle (SDLC). The Snyk AI Security Platform serves as the engine that delivers this Fabric. As the Snyk AI Security Platform puts developers first, it 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.

The Snyk AI Security 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, 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.

Evo by Snyk serves as the platform where Snyk brings its AI security research into practice. Built to address the unique risks of AI-native and agentic applications, Evo provides a foundation for AI Security Posture Management (AI-SPM), including capabilities such as AI Bill of Materials (AI-BOM) analysis, model and agent visibility, risk registries, threat modeling, and red teaming techniques to address risks like model jailbreaking. Evo translates insights from Snyk Labs research into actionable controls and workflows, shaping how AI security is applied across the platform while contributing to the evolution of broader AI security practices across the industry.

In parallel, Snyk Labs is advancing research into securing AI agents and their interactions in complex, real-world environments. As organizations move from experimentation to operational AI, this work informs Evo by Snyk, helping translate emerging agentic security risks into practical protections and workflows designed for AI-native systems.

Finally, Snyk Studio delivers security directly into AI-assisted development. It provides the standardized interface that allows AI coding assistants and agentic tools to incorporate Snyk's security intelligence and policy logic at the moment code is generated and modified. Through this integration, teams can secure code at inception, guiding AI tools toward safer outputs from the first prompt, while also enabling intelligent remediation that helps developers eliminate security debt at scale by combining the power of Snyk and AI to find and fix existing vulnerabilities at unprecedented speed. The result is security embedded natively in AI-driven workflows, without disrupting developer velocity.

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 capabilities** 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.

Snyk has introduced the Prescriptive Path to Operationalizing AI Security, designed to make AI security actionable with the Snyk platform.
This opinionated operating model helps organizations apply security capabilities in a thoughtful sequence as AI adoption reshapes how software is built. Ultimately, this helps teams build fast and fix faster with confidence by reducing risk in software development, enabling faster innovation, and helping them efficiently deliver secure software.

The Snyk platform at a glance

The Snyk AI Security 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. The Prescriptive Path is organized into three strategic phases:

- **Phase 1: Stabilize (Steps 1-2):** Eliminate security blind spots and stop the bleeding by establishing foundational visibility and "Secure at Inception" guardrails.
- **Phase 2: Optimize (Steps 3-4):** Focus on what matters and fix at machine speed by prioritizing exploitable risks and leveraging AI-accelerated remediation.
- **Phase 3: Scale (Steps 5-6):** Govern the program and deploy autonomous defense by establishing automated standards and preparing for an agentic future with Evo.

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 delivers faster, smarter security without disrupting how developers work. It is powered by AI-driven capabilities like **Snyk Assist, Snyk Agent Fix, and Snyk Studio**.

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.

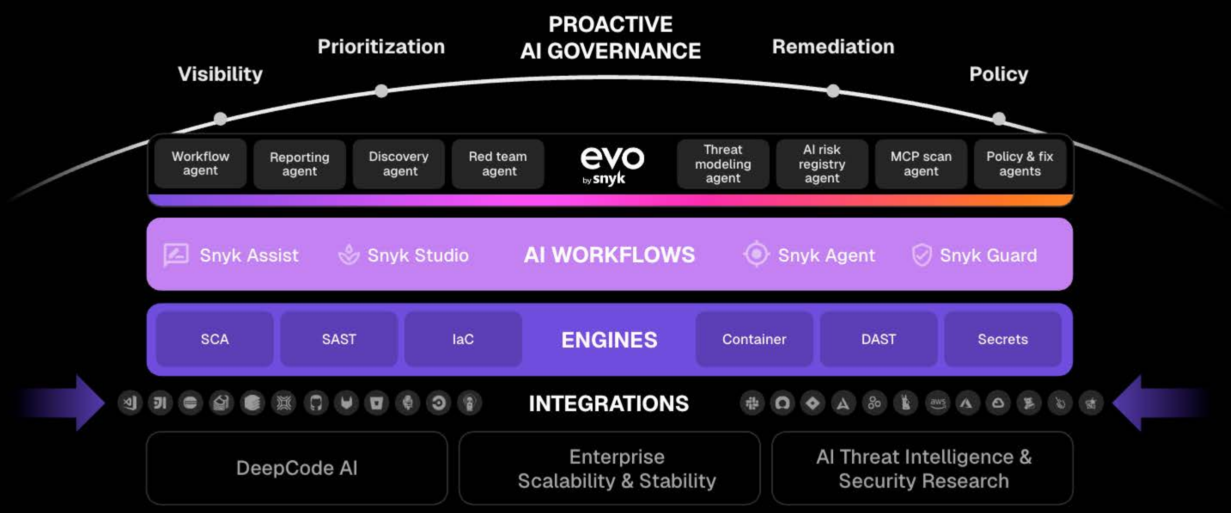
With enterprise-grade coverage, intelligent automation, and seamless developer experience, the Snyk AI Security Platform brings consistency, speed, and trust to modern software delivery. Designed to provide teams with the tools they need in the context they want, the platform empowers you to scale your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

The result:

- **Accelerated security:** A frictionless developer experience 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.

The Solution

The Snyk AI Security Platform



Visibility

Prioritization

PROACTIVE AI GOVERNANCE

Remediation

Policy

Workflow agent

Reporting agent

Discovery agent

Red team agent

evo by snyk

Threat modeling agent

AI risk registry agent

MCP scan agent

Policy & fix agents

Snyk Assist

Snyk Studio

AI WORKFLOWS

Snyk Agent

Snyk Guard

SCA

SAST

IaC

ENGINES

Container

DAST

Secrets

INTEGRATIONS

DeepCode AI

Enterprise Scalability & Stability

AI Threat Intelligence & Security Research

Snyk core engines: Secure every layer

Eliminating security blind spots is the first step in unleashing AI innovation. Snyk provides total visibility and coverage platform.

Each of Snyk's core products focuses 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, when combined, how the whole platform goes beyond shifting security left and DevSecOps, providing a path to embracing the AI Security Fabric.

Snyk Code

Snyk Code is where secure development begins. Focused on proprietary code, it identifies vulnerabilities such as injection flaws, insecure deserialization, and improper data handling 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 DeepCode AI, 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. This provides critical support for Step 2 (Prevention and AI Guardrails) by seamlessly preventing new issues before and at the point of enforcement, the pull request.

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 like zero-days, 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 in 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 Open Source serves Step 1 (Foundational Visibility), eliminating security blind spots across the AI software supply chain to ensure every dependency is identified and secured.

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, hardened images, 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.

As the majority of AI-driven applications get deployed in containers, Snyk Container provides critical, continuous Foundational Visibility (Step 1) and signals for Step 3 (Strategic Prioritization).

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.

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.

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.

Platform capabilities: 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.

Broad visibility and coverage

The **Snyk platform** provides broad software asset visibility and coverage, laying an essential foundation to help organizations scale application security. Designed for teams building or expanding developer-first security practices, it goes beyond scanning to provide the visibility, context, and governance needed to manage risk effectively from day one.

Snyk automatically discovers and continuously maps the application attack surface, pulling in repositories, packages, container images, and more across your existing toolchains. It enables your teams to build policies that automate tagging, classification, and enforcement based on asset attributes or risk profiles so that governance keeps pace with growth. Teams can define and enforce scanning requirements across code, open source, containers, and infrastructure as code (IaC). Once assets are identified and policies are defined, Snyk Essentials helps ensure critical projects are tested in alignment with business requirements and internal compliance objectives, without relying on manual oversight.

To help teams focus capacity on what truly matters, Snyk adds application and business context to the technical findings produced by Snyk's testing engines. By factoring in asset criticality, business impact, and exposure, we enable more efficient, risk-based prioritization, helping development and security teams align on the highest-value remediation work without getting buried in noise.

Snyk Essentials simplifies the platform adoption, strengthens feedback loops, and builds confidence in security decisions, 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. **Snyk Learn** flips that model, delivering contextual, just-in-time security 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 found in their code. If a Cross-Site Scripting (XSS) issue is found, they're guided to a bite-sized 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 Learn 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** serves as your AI-powered mentor for real-time support and clarification, reinforcing learning and boosting confidence without interrupting the flow. Snyk Learn strengthens security culture, helps teams' compliance needs, and scales developer enablement in a way that's finally built for modern software.

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 insights and powerful ROI metrics.

By pulling real-time telemetry across your entire software asset inventory, including AI tooling, 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 dashboards, saved views, and export-ready datasets 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.

AI workflows: Intelligence across the SDLC

With security teams stretched thin and development moving faster than ever, automation isn't just helpful; it's a core component of 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.

Snyk Assist complements Snyk Learn by helping developers understand secure coding concepts and remediation approaches, drawing on guidance from Snyk Learn content, documentation, and blog resources. 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 provides a scalable way to make security expertise easily accessible to developers, without adding tickets or slowing down delivery.

Snyk Agent Fix

Snyk Agent Fix drives Step 4: AI-Accelerated Remediation by providing developers with "one-click" AI-generated fix suggestions that reduce mean time to remediation (MTTR) by 52%. 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 enforces "Secure at Inception" guardrails directly in AI coding assistants, stopping new risks at the source before they ever enter the codebase. Designed for teams adopting AI-assisted development, Studio enables seamless integration of Snyk's security capabilities into AI-powered IDEs, agentic tools, and developer workflows.

Snyk Studio provides the interface that allows AI coding assistants and agentic tools to incorporate Snyk's security intelligence and policy logic directly into AI-powered workflows. It operationalizes AI security by turning Snyk's research and intelligence into real-time guidance and remediation within AI-driven development workflows.

For development, security, and platform teams, Snyk Studio embeds security directly into AI-driven workflows, enabling teams to move fast without introducing new risk. By embedding security at the moment code is created and modified, Snyk Studio enables teams to secure at inception while also supporting intelligent remediation as issues are identified.

Agentic security orchestration with Evo by Snyk

AI is being introduced faster than traditional security tools alone can manage it. Models, prompts, tools, and agents are scattered across teams with no single system of record, inconsistent risk evaluation, and very little runtime control. This leaves organizations exposed to compliance risk, data leakage, and unsafe agent behavior, without clear ownership or accountability. Evo brings structure, governance, and security orchestration to AI at scale.

Evo is the world's first Agentic Security Orchestrator, designed for Step 6 of the path (Orchestration). It provides the autonomous, machine-speed defense required to secure AI-native systems. Built for teams adopting AI-driven development and automation, Evo provides the visibility, governance, and proactive enforcement and controls needed to manage dynamic risk across datasets, models, agents, APIs, MCP Servers, and connected systems through a system of orchestrated agents.

Discovery is foundational to AI security since the largest and fastest-growing AI risks surface in code, where every model, agent, and workflow comes to life. This is the starting gate as Evo continuously inventories and maps AI assets, including models, agents, and dependencies, giving organizations comprehensive insight into their AI attack surface. It anchors risk management with structured guardrails, AI red teaming, threat modeling, and policy orchestration that adapt as systems evolve, not just at discrete checkpoints.

Evo brings together relevant signals and deep context from the broader Snyk platform to help teams prioritize risk intelligently, enforce policies consistently, and continually improve their security posture.

For security engineers, AppSec leaders, and platform teams, Evo delivers a unified view of AI security that scales with development velocity. By translating emerging AI risks into actionable governance and automated workflows, Evo helps organizations confidently adopt and operate AI-native systems without compromising control over risk.

Platform in action: Empowering developers and security teams

Seeing the Snyk Platform in motion helps bring its impact into focus. In practice, secure development doesn't follow a single path. Teams work across a mix of AI-assisted and traditional workflows, and Snyk is designed to support both without friction.

AI-assisted development: Secure at inception within AI workflows

In an AI-assisted workflow, a developer begins writing code in their IDE using an AI copilot equipped with Snyk Studio. As the AI generates code, Snyk's security intelligence is applied at the moment of creation, guiding the copilot toward safer outputs from the first prompt. When insecure patterns or risky dependencies are introduced, Studio enables issues to be identified immediately and, where appropriate, agentically fixed before the code is even presented to the developer. Security is built in at inception, directly embedded into the AI-driven workflow, allowing developers to move quickly without introducing new risk or downstream rework.

IDE-based development: Frictionless security in developer flow

In a parallel workflow, another developer manually writes code in their IDE. As they work, Snyk Code scans continuously in real time, surfacing issues directly in context. When a vulnerability is found, the developer can apply a validated fix generated by the Snyk Agent Fix without needing to file tickets or interrupt the workflow. The same process applies to open source dependencies. If an insecure library is introduced, Snyk Open Source determines whether the issue is reachable and recommends a safe upgrade before the code is committed or merged.

As code moves through CI/CD, Snyk continues to apply security controls consistently across both workflows. Policies are enforced automatically, and risk-based prioritization helps teams focus on what matters most. Powered by the Snyk Risk Score, prioritization combines exploitability signals such as EPSS and reachability with application-level and business context to guide developers and security teams toward the highest-value remediation work.

From a security team perspective, visibility spans the entire process. If a business-critical application has not yet been tested dynamically, the team can quickly assess it using Snyk API & Web to validate runtime exposure and confirm that customer data remains protected. Over time, Snyk Analytics provides a clear view into fix velocity, policy adherence, and platform adoption, enabling teams to measure progress, report outcomes, and continuously improve their secure development practices.

Together, these workflows form a continuous cycle of detection, prioritization, remediation, and governance that flows through the Snyk Platform, helping organizations move faster, stay secure, and make smarter decisions at every stage of software development.

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 developers' hands 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 provides 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.

Let’s get to work

Software moves fast, and security needs to move with it. The Snyk platform is designed to build trust at AI speed. With it, enterprises move from tactical, reactive scanning to a program built on sustainable governance and AI-driven resilience. Whether you are stabilizing your AI supply chain today or deploying autonomous orchestration for the future, Snyk ensures you can safely unleash AI innovation.

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 Security Platform in action.