

UNVARNISHED REVIEWS

Snyk vs. Checkmarx vs. Veracode: The Application Security Testing Verdict

Unvarnished Reviews Research

Market Position: Security Tools Became Part of the Supply Chain

Application security testing finds flaws in code before attackers do, and the category has widened from a scanner run before release to a layer that sits in the editor, the pull request, the build pipeline, and the open-source packages a project pulls in. AI coding assistants raise the volume of code that needs checking, and the vendors have responded with new products: Veracode acquired Phylum in January 2025 to strengthen detection of malicious open-source code and has announced Package Firewall to block malicious packages, while Snyk bought the AI security firm Invariant Labs in 2025 and describes an AI security business alongside its developer products.

That reach is also a risk. A security scanner runs inside the build pipeline with access to the secrets a build uses, so a compromise of the scanner is a compromise of the pipeline. The March 2026 attack on Checkmarx's GitHub Actions showed it: the group behind the earlier Trivy breach used tokens stolen there to poison Checkmarx workflows, and the malware targeted exactly the credentials a pipeline holds. For a buyer, the vendor's software supply chain is now part of the evaluation.

Ownership and finances differ. Checkmarx has been owned since April 2020 by Hellman & Friedman and TPG in a \$1.15 billion deal, with Insight Partners keeping a minority stake. Veracode has been backed by TA Associates since March 2022, at a reported \$2.5 billion valuation. Snyk is venture-backed, has raised more than \$1 billion, and reported 2025 revenue of \$309 million with a loss of \$189 million. A vendor in cost-cutting mode, a private-equity-owned suite, and a growth-stage platform will behave differently at renewal.

Snyk: The Upside

Snyk is the easiest of the three to adopt. Users rate it 4.5/5 across 136 reviews and score ease of setup 8.9, ease of use 8.7, and ease of administration 8.8, ahead of Checkmarx and Veracode on setup and administration, and ahead of Veracode on ease of use. It integrates with GitHub, Azure Pipelines, Amazon ECR, and AI code editors, and users praise its vulnerability detection and identification. Its largest customer segment is mid-market, which fits teams that want security without a dedicated platform team.

The entry point is free. Snyk's Free plan costs \$0 and covers open-source dependencies, static analysis of code, infrastructure as code, and containers, with limits of 5 projects and 100 code tests a month. Team starts at \$25 a month for development teams of up to 10 developers and raises the limits to 100 projects and 1,000 code tests a month. No other vendor here lets a team run a real pilot without a sales call.

Enterprise pricing is flexible, if you can model it. Enterprise is a credit-based platform in which one credit equals \$1 and each capability draws from the balance at a set rate: code and open-source scanning cost 1.0 credit per active contributor per day, and container scanning costs 0.33 credits per monitored image per day. Credits are pre-purchased for the contract term, can be topped up mid-contract, and usage beyond them is invoiced afterward. A team with a mix of products can spend only on what it uses.

Snyk: The Downside

Cost climbs with scale. Users name cost increases at scale among their complaints, and Vendr reports overage fees of \$50-\$120 per extra developer per month, renewal escalators of 5%-10%, and implementation that typically runs \$5,000-\$25,000. Vendr's benchmark for Team list pricing is \$52-\$98 per developer per month, which does not match the \$25 starting price on Snyk's plans page, so confirm the unit and the cap in writing. The Enterprise credit model also makes the bill depend on how often contributors are active.

False positives and interface clutter are consistent complaints. Users cite false positives and poor interface design among their top criticisms, and a small number of public reviews describe code flagged as unsafe that had been correctly sanitized. Users report about three months to implement and about 12 months to see a return.

A June 2026 restructuring cut about a fifth of the company. A UK company filing says Snyk cut approximately 203 employees, about 20% of its global workforce of around 990, across the US and Israel, with an expected cost of up to \$13.8 million. The filing gives the reason as "to further increase operational efficiencies and streamline expenses." Revenue grew 11% to \$309 million in 2025, while losses rose from \$169 million to \$189 million. Snyk declined to comment beyond the filing, and the reporting does not say how the cuts affect customers. Ask which support and customer success teams cover your account.

Checkmarx: The Upside

Checkmarx offers the broadest enterprise suite. Checkmarx One bundles static analysis, open-source software composition analysis, infrastructure as code through its KICS tool, API security, container scanning, malicious-package detection, and Codebashing developer training, and it can be deployed as software as a service or self-hosted. Its largest customer segment is enterprise, and Salesforce is an early investor and partner, working with Checkmarx on AppExchange security reviews.

Users rate it well in the enterprise review pool and describe support as a strength. Checkmarx scores 4.5 across 525 reviews on Gartner Peer Insights, the highest of the three, and users describe support as fast, responsive, and reliable. Users report about two months to implement, shorter than Snyk's three, and cite implementation ease and the interface as strengths.

Pricing is at least partly visible. The AWS Marketplace listing publishes 12-month list prices per license: \$1,035 for Start with SAST NG and \$1,564 for Essential, with add-ons from \$240 to \$345 and a three-year option marketed as saving up to 67%. That is more visible than Veracode's pricing and gives buyers a list to negotiate from.

The company is investing in AI. Checkmarx acquired the AI security agent company Tromzo in December 2025 and plans to use its reasoning engine as an intelligence layer across Checkmarx One.

Checkmarx: The Downside

Checkmarx's GitHub Actions were weaponized in March 2026. Between 12:58 and 16:50 UTC on March 23, 35 tags of the KICS GitHub Action were hijacked, and Sysdig observed a malicious tag on the ast-github-action as well. Researchers at Wiz attribute the attack to TeamPCP, the group behind the Trivy compromise, and believe a compromised cx-plugins-releases service account published the malicious tags. Two OpenVSX editor extensions, cx-dev-assist 1.7.0 and ast-results 2.53.0, were also compromised. The malware harvested environment variables, SSH keys, secrets from runner memory, cloud metadata credentials, and Kubernetes tokens, and tried to persist through privileged Kubernetes pods and a hidden backdoor. Checkmarx published a security update, and the repository was reinstated at 19:24 UTC with the maintainers saying "The issue is resolved now." Wiz observed that the malicious extension versions were still present when it wrote its report. Any team that ran the affected actions in the window should rotate every secret those pipelines could reach and pin actions to full commit hashes.

Contract terms are strict. The AWS Marketplace listing sets a minimum deal of \$30,000 for one year or \$90,000 for three, adds a Premium Service Package priced at the higher of 20% of the software fee or \$10,000 a year, and offers no refunds. Add-ons can only be bought alongside a base product. Vendr reports 3%-5% annual increases on multi-year contracts and advises negotiating longer auto-renewal notice periods.

The review pool is thinner and older. Users rate Checkmarx 4.2/5 across 49 reviews, and the public reviews of earlier on-premises versions describe slow scans and installation that required Windows and a SQL database. Reviewers still cite false positives. Those reports may not reflect the current Checkmarx One, but they are the evidence available.

Veracode: The Upside

Veracode is built for programs with many applications. Pricing by application, scan type, and frequency, modules for static, dynamic, and open-source testing and manual penetration testing, and a central dashboard for application risk, compliance, and scan history suit a security team that owns a portfolio of applications and reports on it. Users praise its security and vulnerability detection, and Gartner Peer Insights users highlight strong static and dynamic testing that catches vulnerabilities early and easy integration with pipelines.

Ratings diverge by source in its favor. Veracode scores 4.4 across 434 ratings on Gartner Peer Insights, in line with Snyk's 4.4 across 236, while the 3.8 across 26 reviews elsewhere comes from a far thinner base.

The vendor reports momentum. In February 2026, Veracode said annual contract value rose 81% year over year in the fourth quarter of 2025 and that more than 130 organizations became customers in that quarter. Those are company-reported figures, not independent ones. It also says it is a Leader in the Gartner Magic Quadrant for Application Security Testing and the Forrester Wave for static analysis.

The cheapest entry in purchase data. Vendr's median buyer pays \$23,774 a year across 87 purchases, in a range of \$9,840-\$143,693, with average savings of about 18%.

Veracode: The Downside

Users score ease of setup and product direction lowest. On the 26 reviews available, users give Veracode 6.3 on ease of setup and 6.3 on product direction, against 8.9 and 8.5 for Snyk, and 7.3 on ease of use against 8.7. The sample is small, so treat the gap as a signal and not a measurement.

Scan speed and noise are the recurring complaints. Users on Gartner Peer Insights report many false positives, including flags on test libraries and development dependencies, slow scans on large monolithic repositories that can delay merges, and a cluttered interface with settings that are hard to find. On the smaller review pool, users name expense and a lack of information as the main cons.

Pricing is opaque. Veracode publishes no price list, and a third-party analysis estimates minimums of about \$15,000 a year for static analysis, \$12,000 for open-source composition analysis, and \$20,000 for dynamic testing, with no self-service or monthly option. Vendr reports annual increases of 5%-10% and recommends negotiating growth terms, overage rates, and annual true-ups up front.

Platform Ratings at a Glance

Platform	G2 Rating	G2 Reviews	Gartner Peer Insights	Trustpilot	Note
Snyk	4.5 / 5	136	4.4 / 5 (236 reviews)	3.0 / 5 on 5 reviews, too few to treat as meaningful	Highest setup and admin scores; June 2026 restructuring
Checkmarx	4.2 / 5	49	4.5 / 5 (525 reviews)	No meaningful Trustpilot presence identified	Highest enterprise review count; March 2026 GitHub Actions compromise
Veracode	3.8 / 5	26	4.4 / 5 (434 ratings)	No meaningful Trustpilot presence identified	Thin G2 base; setup and product direction scored 6.3

The ratings diverge more than in most comparisons. Snyk leads the smaller review pool and Checkmarx leads the larger enterprise pool, and Veracode sits at 3.8 on 26 reviews but 4.4 on 434 ratings, so the source matters as much as the score. None of the gaps should decide the purchase by itself; the Checkmarx supply-chain attack, the pricing unit, and each vendor's scan speed and noise carry more decision weight.

Pricing (October 2026)

Platform	Entry Tier	Mid Tier	Top Tier	Pricing Model
Snyk	Free, \$0: 5 projects and 100 code tests a month	Team, starting at \$25 a month for teams of up to 10 developers: 100 projects and 1,000 code tests a month	Enterprise, quote-based: credits at \$1 each; code and open source 1.0 credit per active contributor per day; container 0.33 credits per monitored image per day	Per contributor or by credit consumption; credits pre-purchased for the term. Vendr median \$45,030 (range \$13,063-\$182,535)
Checkmarx	Checkmarx One Start with SAST NG, \$1,035 per license a year (AWS Marketplace, 12-month list)	Essential, \$1,564 per license a year	Add-ons: API Security \$276, IaC (KICS) \$240, DevAssist \$300, Codebashing \$345, Containers \$240, Malicious Packages \$276; Premium Service Package at the higher of 20% or \$10,000	Per license, minimum deal \$30,000 (one year) or \$90,000 (three years), no refunds. Vendr median \$60,950 across 34 purchases (range \$26,400-\$205,350)
Veracode	No free tier; no public list	Third-party estimates: static analysis from about \$15,000 a year, open-source analysis from about \$12,000, dynamic testing from about \$20,000	Platform bundles estimated at \$100,000-\$250,000 for 25-100 applications	By application, scan type, and frequency; annual contracts. Vendr median \$23,774 across 87 purchases (range \$9,840-\$143,693)

Snyk's Team price comes from its plans page, and the Enterprise credit rates come from the same page; the Checkmarx figures come from a vendor listing on AWS Marketplace and exclude VAT and withholding taxes; Veracode figures are third-party estimates and Vendr data, not quotes. Vendr's pages cite deal counts that do not reconcile between sections, so treat the medians as directional. Vendr reports typical discounts of 15%-30% for multi-year Snyk contracts, 20%-40% for

Checkmarx deals with 50 or more developers, and about 18% on average for Veracode.

TCO Comparison: 100-Developer, 50-Application Organization, One Year

Scenario: 100 contributing developers working across 50 applications, buying open-source, static, and basic platform capability, at list or benchmark prices before negotiation.

Line Item	Snyk	Checkmarx	Veracode
Platform subscription	Vendr benchmark \$52-\$98 per developer a month: $100 \times \$624 - \$1,176 = \$62,400 - \$117,600$. Credit math at list for code and open source ($2.0 \text{ credits} \times 365 \text{ days} \times 100 \text{ contributors}$) is at most \$73,000	Start with SAST NG $100 \times \$1,035 = \$103,500$; Essential $100 \times \$1,564 = \$156,400$	Third-party platform estimate for 25-100 applications: \$100,000-\$250,000
Implementation and onboarding	\$5,000-\$25,000	Free installation services reported by reviewers; Premium Service Package below	Professional services quoted separately
Premium services or support	Premium support quoted separately	Higher of 20% or \$10,000 of the software fee: \$20,700-\$31,280	Premium support quoted separately
Financial backstop or guarantee	None documented	None documented	None documented
Year 1 total, modeled	\$67,400-\$142,600	\$124,200-\$187,680 at list	\$100,000-\$250,000, estimated

The comparison is less clean than most because the three price in different units, so the same organization lands in different places depending on its mix of developers and applications. At list, Checkmarx costs about 1.8x Snyk's lower figure (\$124,200 against \$67,400) before negotiation, and its Premium Service Package alone adds 20% of the software fee. Veracode's range is the widest because it is an estimate and not a published price. Buyers close lower than list: Vendr's median deal is \$45,030 for Snyk, \$60,950 for Checkmarx, and \$23,774 for Veracode, all well under the modeled totals, which suggests most buyers are smaller than this scenario or negotiate heavily.

Costs the Pricing Table Misses

- **Snyk's overages and credit variability.** Vendr reports overages of \$50-\$120 per extra developer per month, and Enterprise credits are consumed per active contributor per day, so a surge in commits raises the bill. Negotiate overage rates and growth terms up front.
- **Snyk's implementation and training.** Vendr puts implementation at \$5,000-\$25,000, and a third-party tracker adds \$5,000-\$15,000 for instructor-led training and a \$15,000-\$50,000 Jumpstart engagement.
- **Checkmarx's service package and minimums.** The Premium Service Package costs the higher of 20% of the software fee or \$10,000 a year, and the minimum deal is \$30,000 for one year or \$90,000 for three, with no refunds.
- **Checkmarx's add-ons.** API security (\$276), infrastructure as code (\$240), editor assistant (\$300), training (\$345), containers (\$240), and malicious-package detection (\$276) are each priced per license and sold only with a base product.
- **Veracode's modules and services.** Static, dynamic, open-source, and penetration testing are priced separately, bundling reportedly lowers cost by 15%-30%, and professional services, premium support, and overages sit outside the subscription estimates.
- **Escalators.** Vendr reports annual increases of 5%-10% for Snyk and Veracode and 3%-5% for Checkmarx multi-year contracts. Cap them.
- **Incident response labor.** A team that ran the affected Checkmarx actions during the March 2026 window faced secret rotation across every pipeline credential, a real cost of a vendor compromise.

Complexity Comparison

Dimension	Snyk	Checkmarx	Veracode
Implementation	About three months to implement and about 12 months to a return, per users; setup score 8.9	About two months to implement, per users; setup score 8.2; older on-premises versions needed Windows and a SQL database	Setup score 6.3 on a small sample; heavier pipeline integration reported
Admin dependency	Low: ease of administration 8.8	Moderate: ease of administration 8.3; enterprise suite with several modules	Moderate to high: ease of administration 7.4
Learning curve for advanced use	Users cite poor interface design and false positives	Multi-module suite with a broader surface to learn	Users cite a cluttered interface with hard-to-find settings
Integration friction	Lowest: GitHub, Azure Pipelines, Amazon ECR, and AI editors	Broad, but pipeline actions need hardening after the March 2026 attack	Pipeline integration is easy per some users, with slow scans on large monolithic repositories
Scan speed and noise	False positives are a top criticism	Slow scans and false positives reported on older versions	Slow scans on large repositories and many false positives, including test libraries
Vendor supply-chain exposure	No incident identified in the sources	Confirmed: the March 2026 GitHub Actions and extension compromise	No incident identified in the sources

The pattern follows each design. Snyk is the easiest to adopt and the noisiest at scale, Checkmarx is the broadest and now carries a documented supply-chain incident, and Veracode is the most program-oriented and the slowest to set up and run. All three produce false positives, which is a property of the category, so the question is how much tuning each requires.

Red Flags

Every finding below is independently documented and material enough to influence a purchasing decision.

Snyk	Checkmarx	Veracode
• About 203 employees, roughly 20% of the company, were cut in June 2026. A UK filing gives the reason as operational efficiency and an expected cost of up to \$13.8 million, while Snyk declined further comment and the reporting does not describe customer effects. Ask which teams support your account.	• Its GitHub Actions and editor extensions were compromised on March 23, 2026. Attackers hijacked 35 KICS tags in about four hours, and the malware harvested pipeline secrets. Checkmarx published a security update and restored the repository the same day. Rotate any secrets those pipelines could reach and pin actions to full commit hashes.	• Lowest scores on setup and product direction. Users score ease of setup 6.3 and product direction 6.3, from only 26 reviews. Validate with references that match your scale.
• Losses are widening. Revenue grew 11% to \$309 million in 2025 while losses rose from \$169 million to \$189 million. Ask about price stability and the support model on any multi-year commitment.	• Malicious extension versions persisted after the fix. Wiz observed the compromised OpenVSX versions still present when it published. Confirm in writing that all affected artifacts have been removed and replaced.	• Slow scans can delay merges. Users report slow scans on large monolithic repositories and many false positives, including test libraries. Run a pilot on your largest repository and time it.
• Cost rises at scale and the Enterprise bill varies. Users cite cost increases, Vendr reports \$50-\$120 overages per extra developer a month, and credits are consumed per active contributor. Set overage rates and a credit true-up in the contract.	• Contract terms are strict. A \$30,000 one-year minimum, a Premium Service Package of 20% or \$10,000, and no refunds. Negotiate the service package and a longer renewal notice.	• Pricing is quote-only with annual minimums. Third-party estimates put minimums at \$12,000-\$20,000 per module and escalators run 5%-10%. Get itemized pricing and cap increases.

- **False positives and interface clutter lead the criticism.** Users and public reviewers cite both. Pilot on a representative codebase and measure the noise.

- **Evidence on current scan speed is thin.** The public reviews of slow scans and heavy installation come from earlier versions. Test Checkmarx One on your repositories before committing.

- **Growth claims are company-reported.** Veracode reports 81% annual contract value growth in the fourth quarter of 2025; independent confirmation was not found. Weigh it as a vendor statement.

The Decision Framework

Choose Snyk if:

- Your engineers will use the tool daily and you want security in the editor and pull request, with a free tier to pilot before you commit.
- You have modeled the Enterprise credit consumption against your commit patterns and negotiated overage rates and a credit true-up.
- You have asked which support and customer success teams survived the June 2026 restructuring and what the contract promises on price stability.

Choose Checkmarx if:

- You are an enterprise that wants static-analysis depth, a broad module suite, and developer training in one platform, deployed as software as a service or self-hosted.
- You have audited every pipeline that referenced the affected Checkmarx actions, rotated the secrets they could reach, and moved to commit-hash pinning.
- You have negotiated the Premium Service Package and renewal notice terms, and you have tested scan speed on your repositories.

Choose Veracode if:

- You run a portfolio of many applications, report on compliance, and want per-application pricing and a central risk dashboard.
- You have timed scans on your largest repository and can live with the noise and the heavier setup.
- You have itemized pricing in writing, with escalators capped, because Veracode publishes no list.

Key Decision Factors

Design decides where security lives. Snyk puts it in the developer's workflow and starts free. Checkmarx offers a broad enterprise suite that you can deploy as software as a service or on your servers. Veracode organizes security around the application portfolio and the program that governs it.

Audience decides which one fits. Snyk suits engineering-led teams, Checkmarx suits enterprise security organizations that want one platform, and Veracode suits compliance-driven programs with many applications.

Price depends on the unit, and the unit is different for each. Vendr's medians put Snyk at about \$45,000, Checkmarx at about \$61,000, and Veracode at about \$24,000, but a 100-developer, 50-application organization models at \$67,400-\$142,600 for Snyk, \$124,200-\$187,680 at list for Checkmarx, and an estimated \$100,000-\$250,000 for Veracode. The Checkmarx supply-chain compromise and Snyk's restructuring add risk costs that no price list shows.

The Bottom Line

- An engineering-led team should pilot Snyk on the free tier, model enterprise credits against real commit volume, and ask what the June 2026 cuts changed in support before signing multiple years.
- An enterprise security team should evaluate Checkmarx only after confirming its remediation of the March 2026 compromise in writing, and should negotiate the service package and notice terms.
- A compliance-driven program should shortlist Veracode, time its scans on the largest repository, and get itemized, capped pricing.

No tool in this comparison is a clean win. Snyk is the easiest to adopt and the vendor most visibly in cost-cutting mode, with enterprise pricing that depends on how often your people commit code. Checkmarx has the broadest suite and the most serious documented security event, and its contract terms are the strictest. Veracode suits a portfolio and a compliance program, and its setup and scan speed are the weakest of the three. Every vendor here carries real pricing friction. The choice is which risks and costs your team can absorb.