Checkmarx vs Veracode

A vendor-neutral technical comparison for security teams | March 2026

konvu

konvu.com/compare/checkmarx-vs-veracode

TL;DR Checkmarx scans source code with a customizable query engine (CxQL). Veracode scans compiled binaries in a managed cloud service with no custom rules. Teams with dedicated AppSec engineers tend to prefer Checkmarx. Teams that want managed accuracy with minimal maintenance tend to prefer Veracode.

Head-to-head overview

Category	Checkmarx	Veracode
Origin	SAST-first (2006), expanded to 10-scanner platform (Checkmarx One, 2021)	Cloud-native from inception, binary/bytecode analysis, managed SaaS-only
SAST approach	Source-code analysis via CxQL query engine. No compilation required. Customizable rules	Binary/bytecode analysis. Compiled artifacts uploaded. No custom rules. Centrally managed engine
Custom rules	CxQL (C#-derivative), Corp/Team/Project scoping, AI Query Builder for natural language	No custom SAST rules. Custom security policies and severity mappings only
Scan speed	Incremental scanning (changed files only), Fast Scan mode (up to 90% faster). Slow on large monorepos	Pipeline Scan: median 90s. Policy Scan: median 8min. Binary upload adds overhead. No incremental scanning
SCA	20 package managers, Exploitable Path Detection, 420K+ malicious package DB, container scanning	~11 ecosystems, Vulnerable Method Analysis, Package Firewall (OPA/Rego), described as 'average'
Enterprise	Cloud, on-prem, hybrid. SSO (SAML/OIDC/LDAP). FedRAMP Ready at High (ATO pending)	Cloud-only. SSO (SAML 2.0). FedRAMP Moderate ATO (July 2022). StateRAMP authorized

What independent benchmarks show

Source	Metric	Checkmarx	Veracode
OWASP Benchmark	Java test cases (2,740)	Tested but anonymized. Default config flags dead code (inflates FPs)	Tested but anonymized. Best commercial Youden Index ~39%, avg ~30%
G2	User ratings and reviews	4.2/5. False Positive Rate: 6.5/10 (lowest dimension)	4.3/5. Product Direction: 6.3/10 (notably low)
Gartner Peer Insights	Analyst positioning	MQ Leader. High FPs out of box, strong after CxQL tuning	MQ Leader. Managed accuracy, finding inconsistency reported
PeerSpot	Practitioner feedback	'Many false positives requiring manual intervention.' CxQL tuning praised	'Binary upload is the #1 complaint.' UI described as 'clunky and disjointed'

Pricing at a glance

Company size	Checkmarx One (estimated)	Veracode (estimated)
Startup (<20 devs)	$30,000-$59,000/yr minimum deal size. No meaningful free tier	$10,000-$15,000/yr (single module). 14-day DAST Essentials trial only
Mid-market (20-200 devs)	$60,000-$200,000/yr. Per-contributor licensing. DAST and AI are add-ons	$50,000-$150,000/yr. Per-application pricing. Support packages costly
Enterprise (200+ devs)	$200,000-$500,000+/yr. Premium support: 20% of subscription	$100,000-$500,000+/yr. Described as more expensive at scale

When to pick which

Pick Checkmarx when:

- Custom rule authoring needed (CxQL engine, org-specific patterns)
- Source-code scanning required (no build step, no compilation needed)
- On-prem deployment required (cloud, on-prem, or hybrid options)
- Broadest single platform wanted (10 scanners incl. API, IaC, secrets)

Pick Veracode when:

- Managed accuracy with minimal tuning (centrally improved engine)
- Binary analysis needed (scan without source code, IP protection)
- FedRAMP compliance required (full Moderate ATO since July 2022)
- Tiered scan speeds for CI/CD (Pipeline Scan: 90s, Policy Scan: 8min)

Sources: OWASP Benchmark, G2, Gartner Peer Insights, PeerSpot. Full article: konvu.com/compare/checkmarx-vs-veracode

The bottleneck is rarely detection. It's triage. If triage is still the problem, that's what Konvu solves. konvu.com/demo