Checkmarx vs Black Duck

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

konvu

konvu.com/compare/checkmarx-vs-black-duck

TL;DR Checkmarx One is one SaaS platform with SAST, SCA, IaC, container, API, secrets, DAST, and ASPM under one UI and policy engine. Black Duck is a portfolio: Polaris unifies three SaaS engines, but standalone Coverity and Black Duck SCA stay separate for on-prem, air-gapped, and ASIL-D safety-critical work.

Head-to-head overview

Category	Checkmarx One	Black Duck (Polaris + Coverity + BD SCA)
Architecture	Single SaaS platform. One UI, one policy engine, one findings store, one license model	Portfolio. Polaris unifies fAST Static/SCA/Dynamic. Standalone Coverity and BD Hub keep separate UIs and policies
SAST approach	Proprietary CxQL engine. Source-code, no compilation. Same engine in CxSAST and Checkmarx One	Coverity engine: interprocedural, path-sensitive, whole-program data flow. Compile-first for C/C++
SCA depth	Manifest + fingerprint. Exploitable Path reachability for Java/Python/JS/C#. 420K+ malicious packages	Forrester SCA Wave Q4 2024 Leader. KB: 10M+ projects, 3K+ licenses, 317K+ vulns. BDSAs avg 165d ahead of NVD
Custom rules	CxQL (C#-derivative) + AI Query Builder. Corp/Team/Project scoping. Self-service	Coverity Code XM. Customer-authored checkers supported but historically PS-driven
Safety-critical	MISRA, CERT, TS 17961, STIG presets. No AUTOSAR, no ISO 26262, no TÜV certification	Coverity: TÜV SÜD IEC 61508-3, ASIL D under ISO 26262, EN 50128/50657. AUTOSAR C++14
FedRAMP	High Ready (Sept 30, 2025). Pre-Authorization. Targeting High impact level	Moderate authorization initiated Jan 28, 2026. Target 'In Process' June 2026. Not Authorized
Air-gapped	CxSAST on-prem only. No purpose-built SKU. Modern ASPM/Assist features SaaS-only	Standalone Coverity + standalone BD Hub on-prem. Strongest air-gapped option in either portfolio

Capability coverage where one side is materially deeper

Capability	Checkmarx One	Black Duck portfolio
IaC	KICS (Apache 2.0 OSS): 2,400+ queries, 20+ platforms	Rapid Scan Static: ~5 platforms (Terraform, CFN, K8s, Dockerfile, Ansible). No published rule count
Container	Dedicated product. Dockerfile hardening + image SCA + first-class registries (ECR, ACR, GHCR, Quay, Artifactory)	Layer-by-layer SCA via BD SCA + BDBA. SBOM. No dedicated Dockerfile-hardening product
API security	Source-code-based discovery. Shadow + zombie API detection. OWASP API Top 10 (incl. 2023)	DAST-only. Accepts OpenAPI/Swagger/Postman/GraphQL specs. No source-based discovery
IAST	Gartner-labeled 'Legacy'. Docs effectively ended at v2.6.1 (May 2020)	Black Duck Seeker. Actively sold. Gartner: 'well-designed tool for IAST testing'
Reachability for SCA	Exploitable Path (function-level) for Java/Python/JS/C#. Attackability (Triage Assist) added 2026	No function-level reachability publicly marketed. Prioritization via BDSA metadata + risk scoring
License compliance	Adequate. Not at Black Duck depth	Industry standard. 3,000+ licenses with encoded obligations. M&A; audit-grade SBOM

Pricing at a glance

Company size	Checkmarx One (estimated)	Black Duck (estimated)
Startup (<20 devs)	$30,000-$59,000/yr minimum deal size	Coverity ~$15,000-$30,000/yr; Polaris per-Application starts higher
Mid-market (20-200 devs)	$60,000-$200,000/yr. Per-Contributing-Developer + Concurrent Scans	Coverity $80,000-$200,000/yr; Polaris bundle $100,000-$250,000/yr
Enterprise (200+ devs)	$200,000-$500,000+/yr. PeerSpot reports ~$500K for ~250 users	$200,000-$500,000+/yr. Vendr: expansion uplifts trend higher than buyers expect

When to pick which

Pick Checkmarx One when:

- Single platform consolidation (SAST+SCA+IaC+container+API+DAST+ASPM)
- IaC, container hardening, or API discovery breadth matters
- Custom SAST rules required (CxQL + AI Query Builder)
- FedRAMP at High impact level is the target today

Pick Black Duck when:

- Deepest commercial SCA + license compliance for M&A or regulated work
- Safety-critical embedded C/C++ (ASIL D, IEC 61508, MISRA, AUTOSAR)
- Air-gapped or fully on-prem deployment is required
- IAST is a meaningful evaluation criterion (Seeker)