DATASHEET

VERACODE + DRYRUN SECURITY

Hybrid SAST + AI

Detect AI-era code risks that other tools miss, even when running at AI-coding scale.

AI coding tools help teams ship faster, but they also increase the volume and velocity of code changes that require security review. Plus, there is a dangerous coverage gap because traditional deterministic scanners don't detect business logic flaws like authorization issues and broken authentication; studies show traditional scanners miss up to 78% of AI-generated risk. Compounding the problem, most organizations are already experiencing 200% expansion in code volume and coding velocity in the last 12 months.

Security leaders need a way to expand coverage without slowing delivery, while still producing evidence that regulated environments require.

Veracode and DryRun Security have partnered to close this gap. By combining DryRun's Contextual Security Analysis engine with Veracode's industry-leading, highly accurate, deterministic, static analysis engine, enterprise teams can uncover more risk before release, keep pace with AI-assisted development, and produce clear, repeatable evidence for auditors and regulators.

KEY METRICS

181%

Increase in applications with high-severity flaws since 2020.

88%

DryRun's out-of-the-box detection rate in benchmark testing, nearly 2× the closest traditional SAST tool.

23 of 26

Seeded vulnerabilities caught in DryRun benchmark testing, including a broken-auth flaw that pattern-based scanners did not detect.

WHAT LEADERS GAIN

DryRun's Contextual Security Analysis Engine reasons across code intent, behavior, and business logic to identify and verify risks that traditional, pattern-based analysis misses.

Veracode SAST provides consistent, repeatable coverage for well-defined vulnerability classes, with findings mapped to major regulatory frameworks.

Together, Veracode and DryRun Security give teams broader coverage, higher-confidence findings, and stronger evidence for remediation, governance, and audit.

BENEFITS AT A GLANCE

- **Broader coverage** across well-defined vulnerability classes and context-dependent business logic risks
- **Reproducible findings** required for regulatory compliance programs
- **Higher-confidence findings** with fewer false positives
- **Reduced AppSec overhead** from manual triage, rule maintenance, and tuning
- **Increased LLM efficiency** for security coverage that scales with the volume and velocity of AI-assisted development

We don't just secure software. *We secure the future.*

VERACODE

HOW TEAMS WORK FASTER

- **The hybrid Veracode/DryRun solution** automatically reviews code changes and merge candidates (e.g. pull requests) and delivers actionable guidance in GitHub or GitLab, helping developers address security issues before code is merged.
- **Veracode and DryRun** don't require custom rule libraries, reducing operational burden for AppSec teams.
- **The workflow** is consistent with how developers use repositories, so there are no distractions or context switches.

KEY CAPABILITIES

1. **Contextual analysis for AI-era code risk** In addition to typical flaws, DryRun helps identify logic flaws like IDORs and broken authentication issues throughout the PR workflow and SDLC that are difficult to find with traditional static scanning alone.
2. **Static analysis for evidence and governance** Veracode SAST and DryRun provide consistent scanning, with findings mapped to major regulatory frameworks.
3. **Inline PR guidance** Developers receive security feedback in the tools they already use, reducing context switching and speeding action.
4. **Complementary analysis for broader coverage** Together, Veracode SAST and DryRun Security combine repeatable deterministic analysis with contextual reasoning, giving teams broader coverage across established vulnerability classes and business logic risks
5. **Remediation** DryRun provides remediation guidance in pull requests and through its MCP integration, helping developers address findings in GitHub, GitLab, or through AI-native remediation in supported AI coding environments, including: Codex, Cursor, Claude, Windsurf, VS Code.

WHAT VERACODE + DRYRUN UNLOCK TOGETHER

Find code risks that need more context

DryRun helps identify logic flaws, IDORs, and authentication issues earlier in the PR workflow.

Show your work with audit-ready evidence

Veracode SAST provides the repeatable scan records and reporting security leaders need for internal governance and external review.

Expand coverage without adding vendor sprawl

Organizations can bring contextual detection and compliance-ready scanning together under one commercial relationship.

HOW IT WORKS

1. **Code is written or generated**
   Developers build with modern coding tools, including AI assistants or Agentic Development Environments.
2. **Pull requests trigger hybrid analysis**
   Veracode and DryRun analyze code before merge and surface findings directly in the developer workflow.
3. **Veracode SAST provides the compliance baseline**
   Teams get consistent static analysis, cross-file taint analysis, and findings mapped to major frameworks.
4. **Findings power a continuous improvement flywheel**
   Results are fed back to LLMs or agents, improving the quality of generated code with each turn — or surfaced through MCP services for in-workflow remediation guidance.

VERACODE + DRYRUN SECURITY

Ready to strengthen AI-era code security and simplify audit readiness?

With Veracode + DryRun, developers receive feedback in the pull request workflow, AppSec gains broader visibility into harder-to-find issues, and leadership gets repeatable reporting to support audit and compliance needs.

Contact your Veracode representative or schedule a demo.

Learn more at www.veracode.com