



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 2x 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