

NEAR-TERM ROADMAP

Security Infrastructure for Agentic **AI Systems**.

AI coding tools are generating production code faster than teams can review it. Security can no longer be a standalone gate — it must be embedded at every step, at developer speed. CodeSlick and Endure deliver the only combined security and maintainability platform built specifically for AI-generated code.

306

Security Checks

164

AI Detection Signals

5

Languages

<3s

Analysis Speed

“The only platform that secures your code AND maintains it.”

CodeSlick

codeslick.dev · Security & SAST

MCP server security · AI code detection · OWASP 2025

Endure

endure.codeslick.dev · Maintainability Intelligence

Drift detection · Intent tracking · Debt scoring

What Distinguishes Us Today

01

LIVE

AI Code Detection

Industry-First

164 signals detect AI-generated code before it ships: 119 hallucination patterns, 32 LLM fingerprints, 13 heuristics. Know what your AI assistant built — and whether it is trustworthy. No competitor comes close.

02

LIVE

Security at Developer Speed

< 3 seconds · Zero Setup

306 checks — OWASP 2025 (95%), MCP server security (12 checks), secrets detection (38 patterns), SBOM + SARIF export. Instant analysis via WebTool, GitHub App, or CLI pre-commit hook.

03

SHIPPING Q1

Fix with Confidence

Breakability Risk Signaling

AI-generated fixes now carry a Breakability Risk label — Low, Medium, or High. Know before you apply whether a fix is safe or needs manual review. The first SAST platform to bring trust signals to automated remediation.

04

LIVE

Three Surfaces, One Platform

WebTool · GitHub App · CLI

WebTool (instant, free), GitHub App (automated PR analysis), CLI (pre-commit, always free). Security where developers work — bring your own API key. No lock-in.

Built for the AI Era — Not Retrofitted

Legacy SAST (Snyk, SonarQube)

- Pattern matching on human-written code
- No AI code detection or LLM fingerprinting
- Remediation = a list of alerts to review manually
- Security only — no maintainability signal
- Requires enterprise procurement and onboarding
- Probabilistic AI tools — findings differ between runs

CodeSlick + Endure

- ✓ 164 AI detection signals, 32 LLM fingerprints
- ✓ Breakability Risk labels on every AI-generated fix
- ✓ 306 security checks in < 3 seconds, zero setup
- ✓ Security + maintainability — in one platform
- ✓ Free WebTool, GitHub App, CLI — start in minutes
- ✓ Deterministic SAST — auditable, CI/CD-ready

ENDURE · AI Code Maintenance Intelligence · v0.2.0 Certified

What No Security Tool Does

As AI agents contribute code at scale, intent drifts. Endure tracks whether your codebase still does what it was designed to do — detecting divergence before it becomes technical debt or a security gap that slips through undetected.

- **Intent Signature Tracking**
100% of project files mapped and versioned
- **Drift Detection**
Flags design-vs-implementation divergence early
- **Maintainability Scoring**
Quantifies AI code debt before it compounds
- **Audit Trail**
Who changed what — and whether it matched intent

What's Ahead

H1 2026

Prevention Reporting

Demonstrate the ROI of shift-left: track and report what was caught before production, not just what was found after. Designed for security leads presenting to leadership.

H1 2026

Combined Dashboard

Unified CodeSlick + Endure view in one surface. Security findings alongside maintainability drift scores — giving teams a complete picture of their codebase health, not just a vulnerability list.

Q1 · Active

Endure Brownfield Validation

Running Endure on CodeSlick's own JavaScript analyzer (2,669 lines). The product validates itself. Live case study in progress — results to be published.

Start Free. No Setup. Results in Under 3 Seconds.

WebTool · GitHub App · CLI Pre-Commit

codeslick.dev · endure.codeslick.dev · support@codeslick.dev