COYOTE PRESS KIT

Security Scanner for Repositories and AI Agents

One-page brief for journalists, analysts, and partners

Updated February 7, 2026

Dual-surface security | CI-ready SARIF output | Agent risk scoring

What Coyote Is

Coyote is a security scanner designed for teams shipping software with both standard repositories and AI agents. It detects exposed secrets, risky patterns, and permission escalation before those issues reach production.

Who It Serves

- Security teams managing application and AI risk together.
- Engineering orgs that need low-noise findings in CI/CD.
- Leaders who want measurable progress: NEW vs FIXED findings.

Why This Matters Now

Most teams now operate two risk surfaces at once: codebases and autonomous agents. Coyote unifies both into one review workflow so security can move faster without giving up control.

Reporter-Relevant Angles

- Shift from static secret scanning to policy-aware agent governance.
- New AI workflow risk: tool access and permission drift over time.
- Practical security ops framing: prioritize regressions, not raw volume.

What It Scans

- Repositories: source files, configs, and full Git history.
- Secrets: cloud keys, API tokens, private keys, and auth credentials.
- Security smells: weak TLS settings, dangerous eval paths, debug exposure.
- AI agents: prompts, tools, permissions, and runtime guardrail posture.

Notable Capabilities

- Dual-purpose architecture: repository and agent security in one scanner.
- Entropy detection for unknown or custom secret formats.
- Diff-first triage that highlights only NEW and FIXED findings.
- JSON, Markdown, and SARIF outputs for CI and code-scanning tools.
- Runtime policy generation for machine-enforceable guardrails.

Assets Included

One-page overview PDF, product summary from the site, and official Coyote logos.

Suggested Framing

"Coyote treats repository exposure and agent capability risk as one security problem."