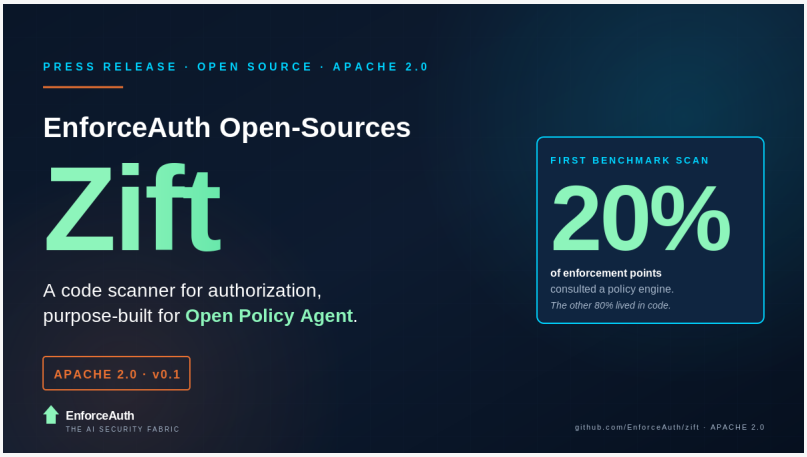
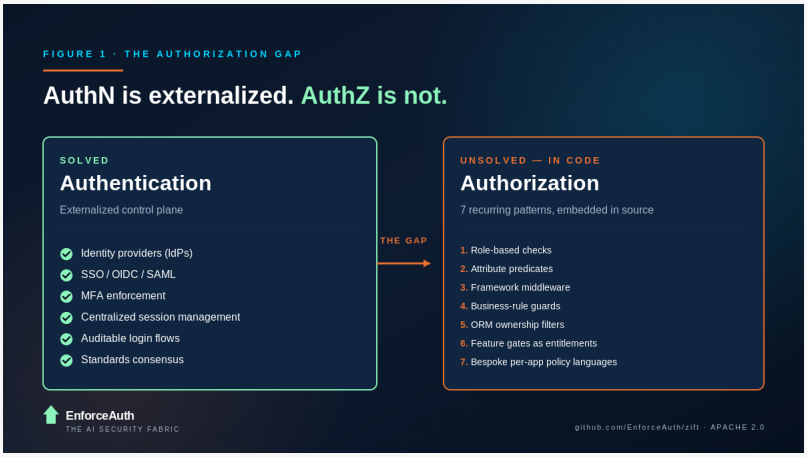
EnforceAuth Open-Sources Zift — A Code Scanner Built to Close the Authorization Gap in Enterprise and AI Systems

First open-source tool to automatically discover authorization decisions across multi-language codebases and emit Rego policy stubs ready for Open Policy Agent.



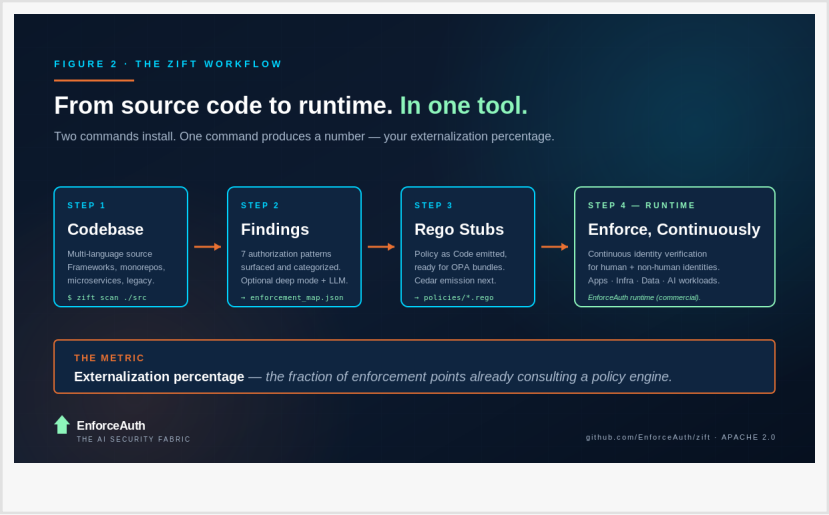


SAN DIEGO, CA, UNITED STATES, May 5, 2026 /EINPresswire.com/ -- EnforceAuth, the AI Security Fabric platform, today announced the open-source release of Zift, a code scanner that automatically discovers authorization decisions buried inside application source code and emits Open Policy Agent (OPA)–ready Rego policy stubs. Zift is licensed under Apache 2.0 with no feature gating, no telemetry by default, and no contractual obligation. The repository is live at github.com/EnforceAuth/zift.

Zift is designed to address what EnforceAuth refers to as the Authorization Gap — the operational surface between authentication, which most enterprises have externalized, and runtime authorization enforcement, which in most enterprises remains embedded inside application code across role-based checks, attribute predicates, framework middleware, business-rule guards, ownership filters in object-relational mapping queries, feature gates, and bespoke per-application policy languages.

In its first internal benchmark scan against a small, well-maintained financial application, Zift reported that only twenty percent of the application's enforcement points already consulted a policy engine. The other eighty percent of authorization decisions were embedded in source code distributed across files, frameworks, and conventions invisible to centralized governance,

audit, or runtime enforcement. EnforceAuth selected the codebase for the benchmark because it expected the externalization percentage to be high.



"Authentication has been solved at the control-plane level. Authorization has not," said Mark Rogge, founder and CEO of EnforceAuth. "If a regulator asks a chief information security officer who can authorize a wire transfer above a certain threshold today, that answer should take ten minutes. In most enterprises we have seen, it takes a multi-week code archaeology project across hundreds of services and produces a probabilistic estimate, not a definitive list. Zift is the first tool that produces a single number — the externalization percentage — and converts the question into a measurable trajectory."

The launch responds to three converging forces in enterprise security architecture: the rise of agentic AI systems acting at machine speed, regulatory frameworks including SOX, PCI-DSS, GDPR, HIPAA, the EU AI Act, and the SEC cybersecurity disclosure rules that increasingly require chain-of-custody evidence for authorization decisions, and the technical consensus forming around Open Policy Agent and the AuthZEN standard for policy enforcement and decision points.

EnforceAuth notes that the non-human-to-human identity ratio in modern enterprises now sits at approximately 82 to 1 — a structural shift that, in EnforceAuth's view, makes static role-based authorization checks insufficient for environments where ephemeral, attribute-rich, machine-speed principals act on behalf of human and organizational identities.

"We could have held this scanner as a proprietary asset," Rogge added. "We chose Apache 2.0 — not source-available, not Business Source License, not open core with a sharp pricing edge — because the discovery step is too important to gate behind a procurement cycle. Every team needs a free, no-strings way to start. The line between the open-source on-ramp and our commercial runtime is bright, and we wrote it down."

Zift is installable in two commands and produces a baseline externalization percentage in one. The repository ships with the complete scanner, the standard parsers, the core rule corpus, the Rego emission engine, and an optional deep-mode integration for local large language models.

Cedar policy emission is on the published roadmap.

EnforceAuth is publishing the scanning methodology with the v0.1 release and inviting the

security community to contribute anonymized scan results so the industry can reason from a real distribution of externalization percentages rather than from intuition.

Installation: brew install enforceauth/tap/zift or cargo binstall zift. First scan: zift scan ./your-codebase.
Repository: github.com/EnforceAuth/zift
License: Apache 2.0

Mark Rogge
EnforceAuth
+1 612-868-7193
email us here
Visit us on social media:
LinkedIn
