ONE-PAGER

Q² Assure

Every finding arrives with its own alibi.

Most scanners hand you a list and ask you to trust it. Q² Assure is a deterministic security review platform — no model participates in any verdict — and every finding is replayed against the exact bytes it cites and challenged for evidence that would refute it, with its prerequisites recorded on the finding and counter-evidence recorded wherever the review found any.

ON THE RECORD

67
detection rules across SAST, secrets, SCA, IaC, container, and post-quantum analysis

554
synthetic findings, each replayed and validated

0
repository code executions

ANALYSIS COVERAGE

01 JS/TS SAST	02 Python/Go/Java/C# SAST	03 SCA (npm/PyPI/Maven/Go)
04 Secrets	05 IaC (Terraform/K8s/CFN)	06 Containers
07 DAST (authorized synthetic targets)	08 Post-quantum (PQC) readiness	09 Governed remediation

WHY IT IS DIFFERENT

Deterministic engine
No model participates in any verdict.

Counter-evidence is first-class
Unresolved assumptions and counter-evidence get their own panel beside impact and attack paths.

Visible 1V–4V
Finder, validator, truth review, and human judgment stay distinct.

Fail-closed replay
Mutation or missing context cannot silently pass as confirmed.

Immutable source identity
Content-addressed manifests bind every claim to exact evidence.

Governed remediation
Minimal-diff proposals, independently re-verified. No auto-write.

WHAT THE DEMONSTRATION DOES NOT SHOW

JavaScript, the Python, Go, Java, and C# engines, the PyPI, Maven, and Go dependency ecosystems, CloudFormation, authorized DAST, the post-quantum checks, and provider-pattern secret matching are real and wired, but they are not exercised by the published demonstration corpus.