ASSURE | APPLICATION EVIDENCE AND ENGINEERING REVIEW

PRODUCT GUIDE · 01 / 04

APPLICATION SECURITY REVIEW AND SOURCE EVIDENCE

Turn every application finding into evidence an engineer can act on.

Assure is an application security evidence and review platform for security and engineering teams. It connects findings to the exact code, checks, uncertainty and human decisions needed for an owned engineering handoff.

The moment

Priya is reviewing a release. The queue contains a possible injection weakness and a cryptographic warning. Her manager asks which one changes the release decision. Assure helps Priya open the source, challenge the claim and record a next step engineering can follow.

Who uses it and where

Application-security analysts, developers, engineering leads and CISOs use the browser console to review nominated repositories and frozen source snapshots. A snapshot is a fixed version of the files: the review can return to the same evidence even after a branch changes.

BRING
Approved source access and a named repository revision

LEAVE WITH
Findings linked to files, lines and a fixed source snapshot

BRING
An agreed analysis scope and configured providers

LEAVE WITH
Validation and replay results, coverage limits, and software and crypto inventory

BRING
A reviewer, engineering owner and review question

LEAVE WITH
A recorded decision, accountable handoff, remediation plan and audit context

The workflow

Authorize and capture the source. Review findings and coverage. Open Evidence to inspect cited code, Investigate to examine the proposed route, and Review to record the human decision. Assign the work, prepare a remediation plan, then examine fresh evidence after a change.

Why consider Assure

The buying question is whether a colleague can reproduce the basis of the finding and continue without reconstructing a conversation. Assure keeps the source reference, validation, uncertainty and handoff together so that review is inspectable.

WHAT THIS ENABLES

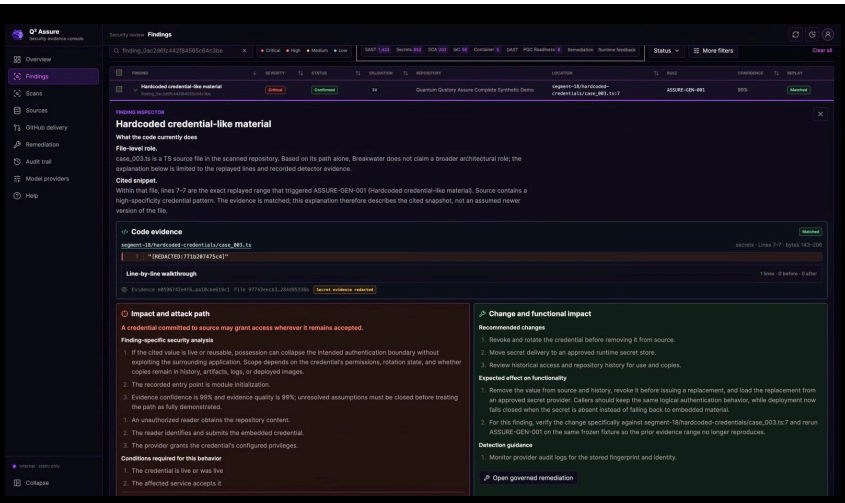
The release discussion starts from a finding someone can examine, with a specific engineering question and an owner.

ASSURE | APPLICATION EVIDENCE AND ENGINEERING REVIEW **PRODUCT GUIDE · 02 / 04**

APPLICATION SECURITY REVIEW AND SOURCE EVIDENCE

The source resolves the first argument

Priya opens the exact source snapshot, checks the cited line and separates what the detector found from what still needs independent review.



Assure interface overview from the recorded demonstration. The full frame shows the finding, exact source evidence, replay context and remediation analysis together; it is a product example rather than proof of runtime exploitability.

A practical walkthrough

Select the scan and open a finding. Inspect the cited line, snapshot and replay result. Move to Investigate for the proposed route and its missing relationships. In Review, record the conclusion and why. Name the engineer and the next check.

Read the cryptographic use in context

A key-generation call establishes that a pattern is present in the reviewed source. Ask what the key does, where it is used, which services depend on it and which stored formats must remain readable. That context determines a meaningful migration task.

Tip for a sparse result

Check completion, filters and coverage before reading an empty list as reassurance. A missing relationship or unavailable replay is an open review question. Keep it visible in the handoff.

WHAT THIS ENABLES

A reviewer can show the source, explain what the check establishes and state the missing evidence that would change the decision.

ASSURE | APPLICATION EVIDENCE AND ENGINEERING REVIEW PRODUCT GUIDE · 03 / 04

APPLICATION SECURITY REVIEW AND SOURCE EVIDENCE

The finding becomes owned engineering work

Priya uses the major workspaces for one continuous job: decide what the evidence warrants and prepare a verifiable next step.

CAPABILITY
Source intake and snapshots

WHAT THE TEAM USES IT FOR
Name the authorized source and preserve the exact version under review.

CAPABILITY
Findings and validation

WHAT THE TEAM USES IT FOR
Inspect deterministic or provider findings, replay source evidence, and retain confirmed, refuted and unresolved outcomes.

CAPABILITY
Investigation and threat models

WHAT THE TEAM USES IT FOR
Review entry points, relationships, sensitive operations and gaps. Modeled routes remain conditional.

CAPABILITY
Software inventory or software bill of materials (SBOM)

WHAT THE TEAM USES IT FOR
Examine components, dependency context and advisory associations within recorded coverage.

CAPABILITY
Cryptographic inventory or cryptographic bill of materials (CBOM)

WHAT THE TEAM USES IT FOR
Locate cryptographic uses and plan post-quantum review with algorithm role and source context.

CAPABILITY
Coverage

WHAT THE TEAM USES IT FOR
Inspect supported analysis, skipped or failed work and limits affecting the conclusion.

CAPABILITY
Review, assignment and history

WHAT THE TEAM USES IT FOR
Record a reason, allocate work, compare scans and preserve the decision trail.

CAPABILITY
Remediation, delivery and reports

WHAT THE TEAM USES IT FOR
Prepare changes and verification, review delivery context and export an evidence-backed report. Execution depends on the authorized path.

Reduce repeated work with available controls

Filter related findings and use bulk assignment for up to 100 selected findings, with an owner, due time and rationale. The batch checks for stale records and does not change truth or severity. Personal category tags help organize work; they are not a shared risk-acceptance taxonomy.

Give the reason a repeatable shape

Record the decision, evidence, unresolved assumption, owner, next check and review trigger. Reuse that structure in the rationale field. AI-suggested categories or wording should remain drafts for human review; automatic approval from similar prose is not an established workflow.

WHAT THIS ENABLES

A finding reaches an engineer with enough evidence to act, while organization and assignment remain separate from confirmation.

ASSURE | APPLICATION EVIDENCE AND ENGINEERING REVIEW PRODUCT GUIDE · 04 / 04

APPLICATION SECURITY REVIEW AND SOURCE EVIDENCE

The next scan preserves the reason

Priya begins the repeat review with what changed while preserving the reason behind the earlier decision.

1 **Carry the source decision into the next scan**

Assure provides a read-only comparison for scans of the same repository, including new, persistent, reopened and no-longer-matched findings. Comparison uses rule and source-location identity and can report ambiguity. Code movement and coverage changes affect interpretation: disappearance from a result is not, by itself, proof of a tested fix.

2 **Keep repeated decisions reviewable**

Suppression changes workflow visibility while preserving underlying truth and rationale in audit history. An identical finding record can retain its state when scanned again. A changed snapshot or finding identity is not a general policy for carrying risk acceptance forward. Review current evidence and link the earlier decision where appropriate; do not substitute suppression for a time-bounded exception process.

3 **Prove the configured operating boundary**

Agree source permissions, supported languages and engines, model use, retention and delivery controls. The documented evaluation centers on static source review. Candidate routes and replayed source evidence do not establish a running application's exploitability. Repository changes require a separately authorized, configured path and fresh verification.

4 **Hand engineering evidence to the wider process**

Keep build, deployment, ticketing and scanner workflows in place. Pair source review with Secure infrastructure evidence through an agreed service and deployment mapping. SOAR may support the operational investigation; verify the actual integration and access boundary.

5 **Make the adoption decision**

Choose one repository and an agreed case set including a known issue, an uncertain result and a repeated scan. Measure evidence-finding time, decision quality and handoff effort against the existing process. Use the full Assure book for operating steps and the pilot outline for engagement design.

WHAT THIS ENABLES

The team can reuse context while recognizing a new finding, stale assumption or incomplete verification that deserves another review.