

**PORTFOLIO** | SECURE · ASSURE · SOAR **PORTFOLIO OVERVIEW · 01 / 02**

PORTFOLIO OVERVIEW

Three products for security decisions that must survive scrutiny

Secure sees the infrastructure. Assure examines the application. SOAR governs the response. Together they carry one decision from observation to accountable action.

PRODUCT AND DEFINITION

Secure - infrastructure security evidence

THE DECISION IT SUPPORTS

Identify assets, services, exposure and cryptographic migration questions from authorized observations.

WHAT THE CUSTOMER KEEPS

A scoped inventory, identity confidence, provider context and an evidence-backed handoff.

PRODUCT AND DEFINITION

Assure - application security evidence and review

THE DECISION IT SUPPORTS

Tie application findings to exact source, review outcomes, uncertainty and engineering ownership.

WHAT THE CUSTOMER KEEPS

Source references, validation results, coverage and a reviewable remediation plan.

PRODUCT AND DEFINITION

SOAR - security investigation and governed response

THE DECISION IT SUPPORTS

Connect supplied evidence to investigation, rehearsal, approval, recovery and fresh verification.

WHAT THE CUSTOMER KEEPS

A reproducible investigation, explicit assumptions and a governed next step.

One service, three decisions

A maintenance window begins with an unidentified device. Secure establishes the infrastructure record. Assure examines the nominated application source and cryptographic use. SOAR investigates the operational question and prepares a bounded response. The same service identifier and review window connect the story.

Each product can stand alone

Start with the decision that matters now. Cross-product context depends on explicit asset-to-service-to-repository mapping and configured integrations; a similar name does not establish the relationship.

What the customer keeps

Every stage leaves an inspectable record: accepted input, source and time, evidence or assumption, human decision, accountable owner and the check that proves the next result.

WHAT THIS ENABLES

A business-unit CISO can identify each product, choose the right starting point and ask for the evidence that supports the next decision.

**PORTFOLIO** | SECURE · ASSURE · SOAR PORTFOLIO OVERVIEW · 02 / 02

PORTFOLIO OVERVIEW

Bring the evidence together without losing its limits

A complete business-unit view depends on agreed scope, identity and time. Buying a product does not establish those relationships automatically.

With or without SOAR

Secure and Assure can be evaluated as separate products. SOAR adds an investigation and response workspace; it should not be described simply as the mandatory backend for both. Supported imports can bring estate evidence into SOAR. Automatic Secure-to-Assure synchronization and a unified group risk dashboard are not established by this reader pack. Agree installed integrations and commercial scope during pilot design.

Use a common review window

Scans need not start at the same second. Name the BU, site, service, source revision, collector vantage point and evidence timestamps. For an incident, narrow the time window. For migration planning, agree a freshness threshold and refresh changed records. Keep unmatched assets and stale inputs visible.

KEEP THESE QUESTIONS SEPARATE

Origin: observed, imported, inferred or simulated

WHAT THE LABEL ESTABLISHES

How the claim was produced. A modeled route remains modeled even if approved.

KEEP THESE QUESTIONS SEPARATE

Review: confirmed, refuted or unresolved

WHAT THE LABEL ESTABLISHES

What the available checks support. Refutation rejects a claim; confirmation is limited to the evidence checked.

KEEP THESE QUESTIONS SEPARATE

Action: proposed, approved, executed or verified

WHAT THE LABEL ESTABLISHES

What happened to the change. Approval needs scope and validity; verification needs a fresh check of the intended result.

Read only as deeply as the decision needs

Start with the product one-pager and its evaluation brief. Use the four-page guide to revisit the workflow and the full book for screenshots, operating steps and technical detail. The chapter navigator states the outcome of every chapter. Use the separate pilot outline to agree inputs, owners, success measures and the decision about expansion.

Establish the group reporting boundary

Assign a business-unit owner and access boundary, map shared services explicitly, and agree which summaries group reviewers may see. Report coverage, unresolved risks, accepted exceptions and freshness by business unit. Treat the initial group summary as a governed reporting process until automated cross-unit behavior is demonstrated.

WHAT THIS ENABLES

The group can ask one coherent question while retaining each product record, evidence boundary and accountable owner.