SECURE | INFRASTRUCTURE EXPOSURE AND CRYPTOGRAPHIC READINESS

PRODUCT GUIDE · 01 / 04

INFRASTRUCTURE SECURITY AND CRYPTOGRAPHIC READINESS

See the device. Understand the exposure. Plan the safest next move.

Secure is an infrastructure security evidence platform for asset owners, vulnerability teams and security leaders. It turns authorized local observations into a scoped inventory, reviewable exposure and an owned next step.

The moment

Maya has a short maintenance window. The work order names a camera, but the site team cannot yet say which device that name means or how it was identified. Secure lets her examine observations, confidence and services before deciding what to investigate.

Who uses it and where

BU CISOs, infrastructure engineers, site operators and security architects use the browser console to review authorized evidence from IT, OT and IoT environments. Collectors run within the approved local environment. Visibility depends on placement, enabled methods and the devices that provide evidence.

BRING
A named site, service owner and approved collection boundary

LEAVE WITH
A run-scoped inventory with identity confidence and source context

BRING
An authorized local collector and a demonstrated destination-acceptance path

LEAVE WITH
Reviewable services, software or crypto evidence, provider states and gaps

BRING
A question about exposure, migration or change

LEAVE WITH
A prioritized review and an export or report for the next owner

The workflow

Prepare or pair authorized local collection, confirm destination acceptance, and open the exact named run. Treat the browser file picker as a review-stage control until the deployed parser and acceptance path are demonstrated. Examine identity and vulnerability evidence in their applicable workspaces, then prepare the handoff.

Why consider Secure

The useful distinction is the connection between an asset label and its evidence. Within the applicable named run, reviewers inspect identity and vulnerability evidence in their respective workspaces. Post-quantum cryptography (PQC) samples, attack paths and twin previews are separate evidence contexts unless an installed integration proves the relationship.

WHAT THIS ENABLES

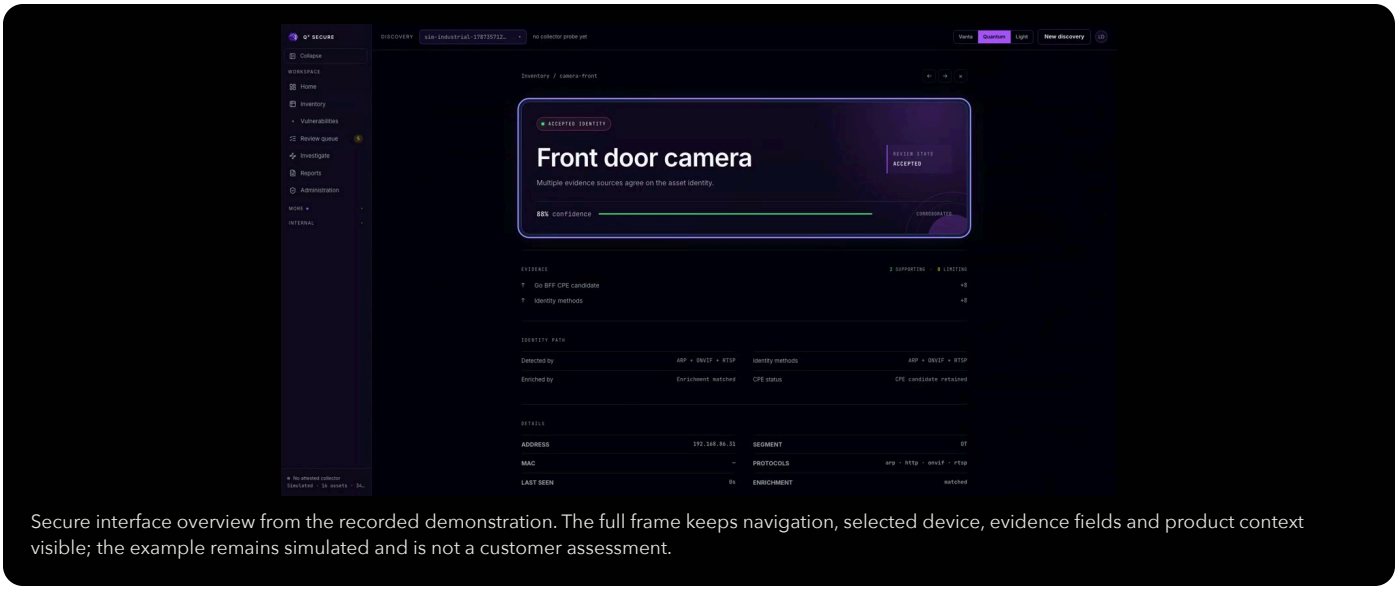
An engineer can explain which asset the record describes, why that identity is credible and what still requires a check.

SECURE | INFRASTRUCTURE EXPOSURE AND CRYPTOGRAPHIC READINESS **PRODUCT GUIDE · 02 / 04**

INFRASTRUCTURE SECURITY AND CRYPTOGRAPHIC READINESS

The device passport changes the conversation

The maintenance request said camera. The passport gives Maya a specific device, the evidence behind its identity and the uncertainty that remains.



Secure interface overview from the recorded demonstration. The full frame keeps navigation, selected device, evidence fields and product context visible; the example remains simulated and is not a customer assessment.

A practical walkthrough

Open Inventory for the selected run and filter to devices needing review. Open a passport, examine observed services and the identity basis, then record the next decision or assign a site check. Export the scoped evidence for the owner who will verify it.

When there are hundreds of similar records

The identity Review Queue includes selected-item Accept, Flag and Assign to me actions. Use them for records whose evidence you have reviewed. A sample may reveal a common issue, but does not confirm every device identity or accept every vulnerability. Keep outliers and weaker evidence separate.

Tip for an apparently empty queue

Check the selected run, completion state, collection coverage and active filters. An empty queue says little if the collector did not observe the intended segment or the relevant provider did not run.

WHAT THIS ENABLES

The reviewer can distinguish a recognizable device from proven exposure and organize repeated identity work without hiding exceptions.

SECURE | INFRASTRUCTURE EXPOSURE AND CRYPTOGRAPHIC READINESS PRODUCT GUIDE · 03 / 04

INFRASTRUCTURE SECURITY AND CRYPTOGRAPHIC READINESS

The evidence connects asset to exposure

Maya moves from the observed device to services, software, candidate vulnerabilities, routes and migration questions without treating them as equal kinds of proof.

CAPABILITY
Discovery and enrichment

WHAT IT HELPS YOU DECIDE
Which assets and services were observed, and which identities need attention?

BOUNDARY TO RETAIN
Quiet devices or devices outside the collector's view may be missing. Confidence is not certainty.

CAPABILITY
Software and crypto inventory

WHAT IT HELPS YOU DECIDE
Which component or cryptographic role needs owner or supplier verification?

BOUNDARY TO RETAIN
Only supported records accepted into the named run describe it; samples remain examples.

CAPABILITY
Vulnerability review

WHAT IT HELPS YOU DECIDE
Which candidates deserve investigation, confirmation or a documented exception?

BOUNDARY TO RETAIN
Database matches and severity do not establish applicability or exploitation.

CAPABILITY
Attack-path analysis

WHAT IT HELPS YOU DECIDE
Which relationships could connect exposure to an important asset?

BOUNDARY TO RETAIN
Projections and candidate routes need their assumptions checked.

CAPABILITY
Exact-run cryptography review

WHAT IT HELPS YOU DECIDE
Which software, cryptography, transport layer security (TLS) or secure shell (SSH) evidence accepted into the named run supports migration planning?

BOUNDARY TO RETAIN
The book uses labeled planning samples. Missing evidence leaves posture Unknown.

CAPABILITY
Candidate paths and supplied model previews

WHAT IT HELPS YOU DECIDE
What could a proposed control change, and what recovery should be prepared?

BOUNDARY TO RETAIN
The recorded edition does not author arbitrary scenarios. Deltas are modeled, not production measurements.

CAPABILITY
Reports and assistant access

WHAT IT HELPS YOU DECIDE
Can another person inspect the source, review state and unresolved question?

BOUNDARY TO RETAIN
External assistant use needs approved access and its own data-handling review.

Make cryptographic planning operational

Inventory the role first: key establishment, signing, certificate use or another function. Add information lifetime, estimated migration duration, service dependencies and the responsible owner. Use those assumptions to prioritize work; an algorithm name alone is not a migration plan.

WHAT THIS ENABLES

The team can turn a technical observation into a review priority, with the dependency, owner and uncertainty attached.

SECURE | INFRASTRUCTURE EXPOSURE AND CRYPTOGRAPHIC READINESS PRODUCT GUIDE · 04 / 04

INFRASTRUCTURE SECURITY AND CRYPTOGRAPHIC READINESS

The owner leaves with a scoped plan

Maya ends the review with a named asset, visible coverage, an owned next check and a decision about whether to expand the scope.

1 **Put collection where it can answer the question**

Choose authorized local collection, a deployment-approved evidence path or a labeled simulator exercise. The current browser Upload bundle and Secure JSON controls stage a reviewed filename; they do not parse it, create an accepted run or populate inventory. Agree allowlists, methods, authorization window and data handling.

2 **Compare the next run without losing context**

Compare new evidence with the earlier run. Vulnerability validation records include an owner, reason and evidence; risk acceptance also needs a review date. Treat the decision as scoped to its recorded run and finding. Do not assume a new run inherits acceptance. Recheck changed identity, firmware, exposure and evidence, and link the earlier rationale when relevant.

3 **Join infrastructure, source and response deliberately**

Use Secure for the infrastructure record and Assure for the nominated application source. Confirm the asset-to-service-to-repository relationship during review. SOAR can use supported estate imports for investigation; verify the actual adapter and identifiers. A continuous shared intelligence view is an integration requirement to demonstrate.

4 **Test the workflow on the customer estate**

Trace one device identity to its observation. Account for collection gaps. Review a repeated-record group and an outlier. Export an actionable finding. Repeat a run and check what changed. For post-quantum cryptography (PQC), agree which evidence can populate the selected workspace and demonstrate the boundary between planning examples and customer observations.

5 **Make the adoption decision**

Nominate a BU owner, one service or network segment, and the question that costs the team time. Use the pilot outline to agree permissions and success measures. Continue with the full Secure book for collection, evidence review, planning and daily operation.

WHAT THIS ENABLES

A pilot produces a reproducible scoped result and an explicit expansion decision, with the operational limits still visible.