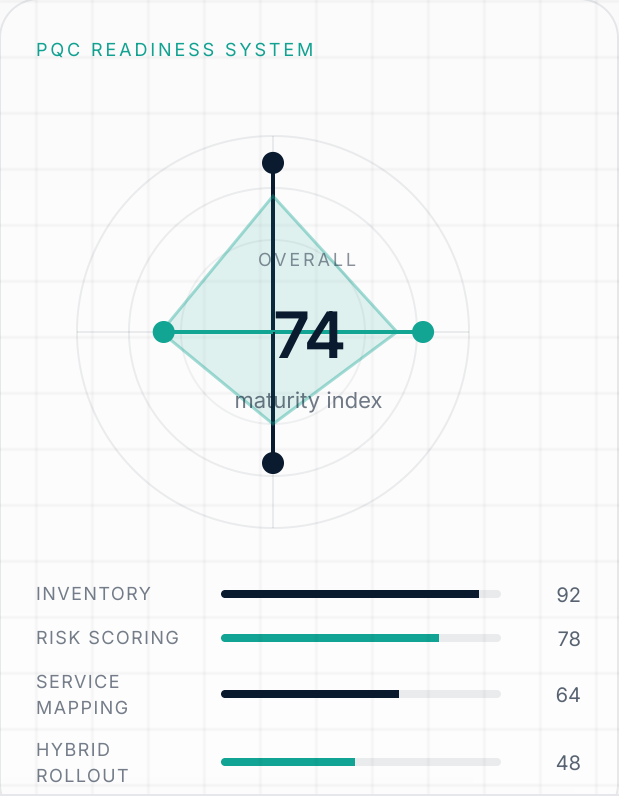
quanterios
cryptographic and ai security and governance

EDITION
Quanterios in practice 02
02 May 2026

OFFICIAL PUBLICATION | WHITEPAPER SERIES

Operating AI Runtime Defense with Quanterios AI

How to deploy inventory, runtime policy, and action validation across live agent and MCP estates.



AIBOM Runtime Evidence

Cookie preferences

Set how Quanterios handles non-essential storage and measurement.

Necessary storage supports security, language, and core site operation. Analytics and any future marketing technologies stay off until you allow them.

Review cookie settings

EDITORIAL BRIEF

Executive summary

AUDIENCE

AI Platform Team, Security Engineering, Model Governance, Risk and Compliance

FORMAT

Quanterios Whitepaper

LENGTH

14 pages

Quanterios AI combines AI inventory, runtime policy, prompt defense, action validation, and evidence generation into one operating surface for agentic systems.

This paper walks through how teams can use the platform in production, from first inventory to runtime enforcement and assurance reporting.

ISSUE MAP

Contents

WHY THIS PAPER MATTERS

Quanterios whitepapers are designed to be carried into investor meetings, buyer reviews, partner conversations, and internal strategy sessions as serious editorial assets, not marketing one-pagers.

SECTION 01

Inventory first: build the AIBOM

WHY URGENCY IS COMPOUNDING

Research	Planning
Procurement	Modernization

The first stage is mapping models, agents, prompts, datasets, tools, MCP servers, and ownership relationships. Teams need to know not only what exists, but what can act, what it can access, and what evidence exists around it.

SECTION 02

Policy second: define allowed behavior

OPERATING MODEL

OPERATING CYCLE

Discover to evidence

01 Discover cryptography everywhere
02 Score posture and exposure
03 Prioritize by service consequence
04 Roll out hybrid migration waves
05 Prove progress with live evidence

Runtime policy turns abstract security expectations into actual gates. Quanterios AI lets teams define which prompts, outputs, tools, and action categories require blocks, warnings, or approvals.

That policy is most useful when it is visible to both engineering and assurance stakeholders, not only hidden in enforcement code.

SECTION 03

Validation third: govern side effects

Prompt injection is only one piece of runtime defense. Teams also need to validate whether the system should be allowed to invoke a tool, alter data, call an external service, or continue a workflow based on current context and scope.

WHERE MIGRATIONS STALL

Late discovery
Hidden certificates, appliances, and supplier code

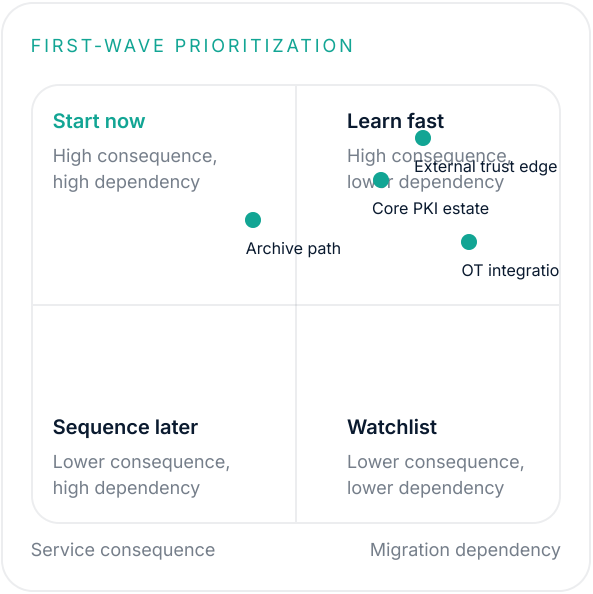
Fragmented ownership
Security, delivery, infra, and compliance see different records

No service map
Findings are not tied to consequence or change windows

No exception logic
Temporary tolerances cannot be reviewed or expired cleanly

SECTION 04

Evidence fourth: keep assurance current



Once runtime controls are active, Quanterios AI makes the resulting control record useful to governance teams. The same platform that sees the live estate can also support review packets and control narratives without parallel manual assembly.

CLOSING SPREAD

From insight to action

KEY TAKEAWAYS

- Runtime defense works best when inventory, policy, and evidence live in the same system.
- Prompt filtering alone is not enough for agentic systems.
- Quanterios AI supports both live enforcement and assurance visibility.

WHAT STRONG TEAMS DO NEXT

NOW

Make the estate visible

Create one living control record across assets, services, owners, and deadlines.

NEXT

Run a first-wave queue

Move the highest-consequence services into a controlled hybrid rollout plan.

THEN

Prove progress

Review migration status and exceptions as an operating program, not a slide deck.

NEXT STEP

Need a runtime-control layer for your AI estate?

Use Quanterios AI to turn runtime policy, action validation, and assurance evidence into one operating model.

Request AI preview

Cookie preferences

Set how Quanterios handles non-essential storage and measurement.

Necessary storage supports security, language, and core site operation. Analytics and any future marketing technologies stay off until you allow them.

Review cookie settings