
USE CASE

Architecture, threats, controls and cloud evidence on one canvas

One canvas joins your architecture, the threats on each component, the controls that answer them and what your live cloud says about those controls.

THE PROBLEM

Our threat model was right on the day it was written, and the architecture moved the next sprint.

The threat model, the scanner and the compliance framework each hold part of the picture, and joining them is an afternoon of manual work. When someone asks for a posture percentage, we can't say what it is out of.

WHY IT MATTERS NOW

60%

of organisations managing risk in silos had a breach,
against 41% of those using integrated GRC automation

Source: Hyperproof 2025

HOW ARIBOT HANDLES IT

1 **Bring in the architecture**

Upload a diagram or compose one on the canvas.

2 **See threats per component**

Each component carries its own threats, derived with STRIDE, PASTA and MITRE ATT&CK.

3 **Follow a threat to controls**

Select a threat to see the controls that answer it and the frameworks they satisfy.

4 **Test against the live cloud**

Connected accounts evaluate controls on real resources, and a scan result outranks a manual assertion.

WHAT YOU GET

- Threats attached to the component they apply to
- Controls linked to their threats and to every framework they satisfy
- Coverage by evidence source, shown beside the score
- Value at risk computed for the diagram in view

SEE IT IN THE DEMO

- An architecture canvas with internet, WAF / load balancer, web app, queue and database components
- A posture header split into code, cloud, dynamic and account coverage
- Counters for components, threats, controls in scope and controls with a result
- Sample figures labelled as an illustrative example, not customer data

See it for yourself

ayurak.com/demos/unified-workbench

€600 per diagram, three regenerations included · free
Starter tier with one diagram