

Aviatrix Harvest and Decrypt Protection

All containment isn't created equal. Five properties separate a small, contained incident from a catastrophic breach. Four more determine whether your data is already leaving. Most security stacks can't demonstrate any of them. Harvest Now, Decrypt Later makes the stakes existential: adversaries record encrypted cloud traffic today, betting quantum computers will break the cryptography. And wide-open egress means the data is already leaving, no quantum required.

Aviatrix Harvest and Decrypt Protection answers both: crypto-agile encryption makes captured traffic worthless, egress governance closes the paths data leaves through, delivered in the fabric, not bolted on, with crypto-agility to adopt post-quantum algorithms as they ship.

STEP 1

Assess Containment Gaps and Harvest Exposure

Aviatrix Harvest and Decrypt Protection begins with the Aviatrix Containment Assessment, Phase 1, a free, self-service 5-minute assessment that tests whether your containment architecture can limit the blast radius of a breach and whether your data is leaving through ungoverned or unencrypted paths. It has two tracks:

1. Containment Path: What Can an Attacker Reach?

- 1. Describe your security stack:** Tick the categories you run in your network: NGFW, security group, service mesh, CNAPP, EDR, identity/MF, SIEM, and WAF.
- 2. Test the five containment properties against your stack:** Determine whether your containment architecture is Path-complete, Identity-aware at L7, Detection-independent, Compute-model agnostic, and Universally Propagated.
- 3. Review containment gaps:** Find what's ungoverned, predict attacker action, and discover documented breaches that exploit these gaps.
- 4. Size your estate:** Inventory your VPCs, Kubernetes clusters, serverless functions, managed services, and partner networks.

Result The Containment Assessment, Phase 1 will evaluate your Provisional Blast Radius: the percent of enforcement domains reachable from one compromised workload.

2. Harvest Path: Is the Data Already Leaving?

- 1. Test four harvest and egress properties:** Assess how your network measures up to standards like being egress-governed, encrypted in transit, key control, and NAT gateway dependency.
- 2. Harvest & egress gaps revealed per property:** Find what's exposed, predict attacker action, and learn what historical breaches happened when that property was neglected.

Result The Containment Assessment will evaluate your Provisional Blast Radius: the percent of enforcement domains reachable from one compromised workload.

STEP 2

Measure the Gaps

After finding the gaps in your network with the Containment Assessment, measure them with the Containment Assessment, Phase 2. This read-only, agentless assessment quantifies your exposure using your own data and produces a priced remediation roadmap your CISO can fund.

- 1. Connect your environment** – Assign a read-only IAM role for visibility. No agents, no topology changes, and no production impact.
- 2. Facilitated analysis** – Aviatrix maps your estate: reachability graph, encryption posture, egress coverage, blast radius per VPC, compliance exposure. Delivered in a structured session.
- 3. Priced roadmap** – The Assessment scores every finding by risk reduction, durability, and cost. One-click remediations are ranked first. Your existing cloud spend already covers much of the transition.

Result The Containment Assessment, Phase 2 will evaluate your environment for egress, encryption, compliance, blast radius, remediation tiers, and key control and produce a Remediation Roadmap that catalogues risk, fixes, and costs.



Receive Five Free Policies

At any point in the journey – after both phases of the Containment Assessment – you can activate five custom encryption and egress governance policies that are free, forever, with no trial or time limit. These policies will lock down your security stack against Harvest Now, Decrypt Later by closing containment gaps and harvest exposure.

Start your journey to crypto agility and quantum resilience with Aviatrix

About Aviatrix

Aviatrix® is pioneering the Cloud Native Security Fabric – the architecture the Containment Era requires. The Cloud Native Security Fabric governs every workload communication path across every cloud, every VPC, every Kubernetes cluster, and every serverless function, from a single policy plane. One rule. Universal propagation. Enforced at the workload, not at a chokepoint. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.