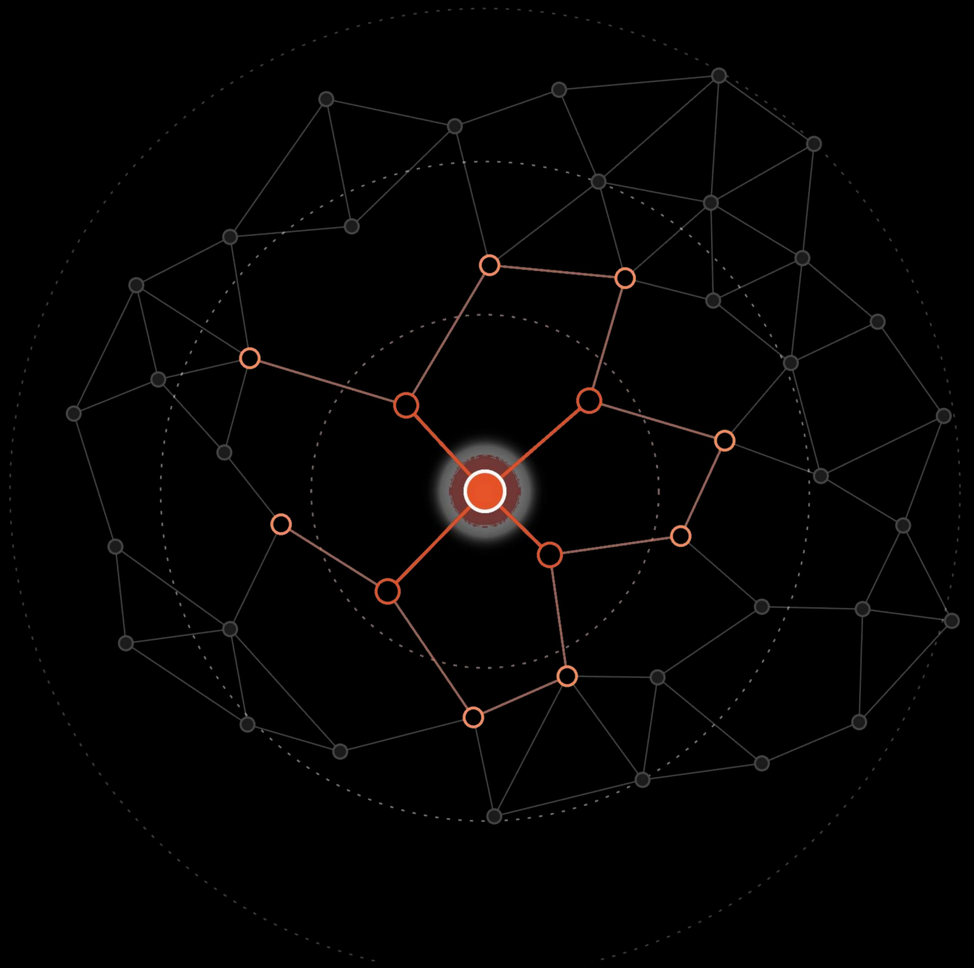
AVIATRIX®

SAMPLE REPORT · HARBORLINE FINANCIAL GROUP (FICTIONAL) · OCTOBER 2026



Containment Assessment

If one workload is compromised, how far can it go?

BUILT ON THE AVIATRIX CONTAINMENT GRAPH

3,140 workloads

612 VPCs

186 cloud accounts

WHAT THIS REPORT DRAWS ON

Controller snapshot · read-only ✓ **Inventory** ○ DNS + flow logs ○ Monitor mode

Perimeter · Blast Radius · Kubernetes · Serverless

CONTAINMENT ASSESSMENT · AT A GLANCE

Three priorities, ranked by what they protect

Each area, and the first step that removes the most risk.

01 · PERIMETER

1,334

workloads leave with nothing inspecting egress

642 NAT gateways · 154 public IPs

FIRST STEP

Configure DCF on the hubs, then threat monitoring

1,640 workloads already egress through Aviatrix FQDN hubs with no threat intel; the densest NAT VPCs follow.

policy change

02 · BLAST RADIUS

812

footholds reach critical systems on RDP/SSH

127 of 146 VPC-to-VPC paths on mgmt ports

FIRST STEP

One management-port policy between SmartGroups

Core Banking Services first: 784 hosts in 26 VPCs reach it, via one 10.0.0.0/8 rule.

policy design

03 · KUBERNETES

84%

of Blast Radius risk touches Kubernetes

38 EKS clusters · 412 nodes

FIRST STEP

Onboard the clusters, production first

Kubernetes SmartGroups per namespace and service; then policy per pod.

onboarding

☆ Ranked by business criticality (AI-inferred) × exposure today. Serverless (04) sits outside every instance count and is covered separately.

Internal Use Only -

01 · PERIMETER

52% of Harborline's egress already crosses Aviatrix

How 3,140 workloads reach the internet today, traced per subnet route.

1,640 workloads
Aviatrix FQDN hubs via TGW
24 hubs · 187 VPCs · 152 K8s nodes



NEXT STEP
Add DCF threat monitoring on the hubs
Names each workload; threat feeds and IPS, then blocking.

1,180 workloads
NAT gateways, no inspection
642 NAT GWs · 311 VPCs · 260 nodes



NEXT STEP
Put the densest NAT VPCs behind DCF
Five VPCs hold 410 workloads.

154 workloads
Direct internet via public IP
11 open to RDP/SSH from the internet



NEXT STEP
Close direct internet exposure
Remove internet-facing management rules today; then move public-IP workloads behind Aviatrix.

LEGACY FQDN GATEWAYS
Retired with the move to DCF; WebGroups carry the domain lists over
24 FQDN gateways · 187 VPCs

NEXT STEP · KUBERNETES
Onboard Kubernetes: per-workload egress control
412 cluster nodes

Not shown: 166 workloads with no internet path or an unresolved route.

Internal Use Only -

02 · BLAST RADIUS

One foothold reaches 22 VPCs on management ports

214 hosts accept RDP/SSH/WinRM from other VPCs.

THE LARGEST BLAST RADII

build-runner-vpc
CI/CD runners · 22 VPCs
pivot 100/100

vpn-access-vpc
same 22 targets
a second source

Shared Kubernetes
Kubernetes · 8 VPCs
pivot 88/100 · k8s

ADMITTED BY

10.0.0.0/8
10.64.0.0/16

Core Banking Services	CRITICAL
prod-payments-vpc	CRITICAL
shared-services-vpc	MEDIUM
Microsoft Active Directory	MEDIUM
Enterprise Service Bus	MEDIUM
stage-app-vpc	MEDIUM
Shared Kubernetes Cluster	MEDIUM

+15 more VPCs

No path crosses an inspection point between VPCs.

WORTH KNOWING

The build runners take no traffic from the internet. Inside the cloud, they reach every production VPC.

THE CROWN JEWEL

784

hosts in 26 VPCs reach Core Banking Services (critical) on RDP/SSH, via one 10.0.0.0/8 rule.

FIRST STEP

One management-port policy between SmartGroups

policy design

THEN

Replace broad 10.0.0.0/8 grants on management ports with identity policy

Paths are inferred from routing and security groups. DNS and flow logs would show which ones carry traffic.

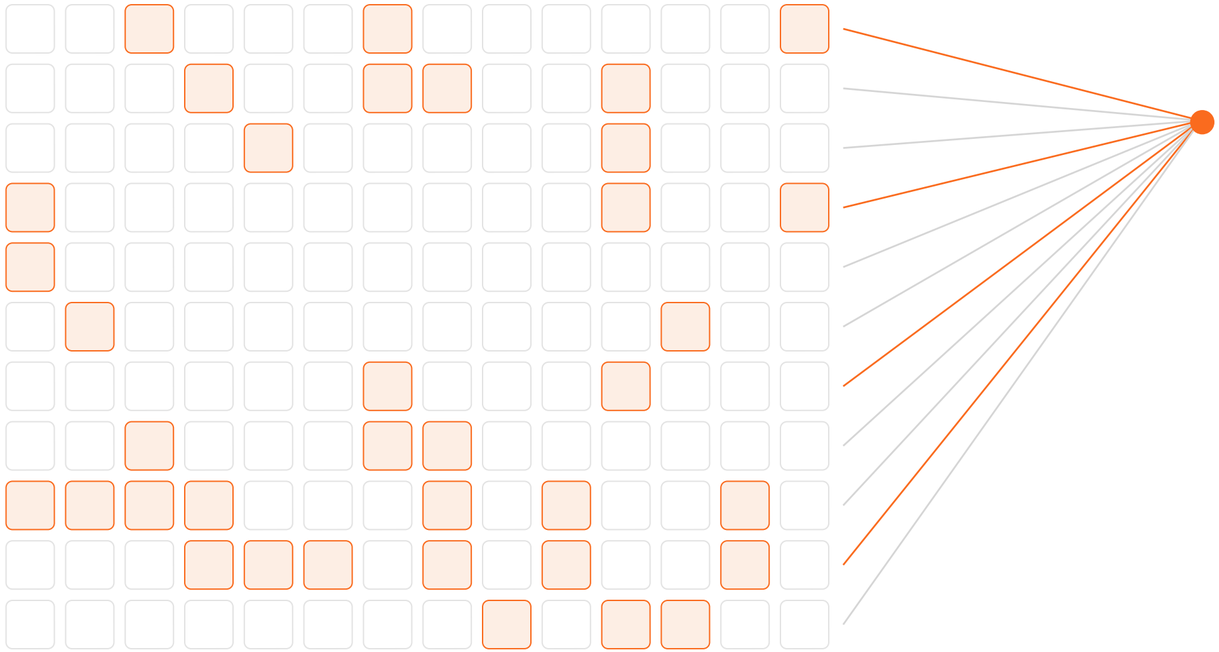
Internal Use Only -

02 · BLAST RADIUS

One SmartGroup policy replaces 2,184 rules

1,262 security groups across 171 accounts, one DCF rule.

TODAY · 2,184 RULES · 1,262 SGS · 171 ACCOUNTS



rule admits RDP/SSH/WinRM from a broad CIDR

Today: edit each rule, in each account.

ONE DCF POLICY

deny RDP/SSH/WinRM between SmartGroups

allow admin tier / PAM → mgmt ports

Monitor first, then enforce.

44.6%

of Harborline's pivot potential, removed.

By closing management ports between VPCs alone.

ALSO URGENT

Close management ports into Core Banking Services

ALSO URGENT

Isolate the build runners: they reach every production VPC

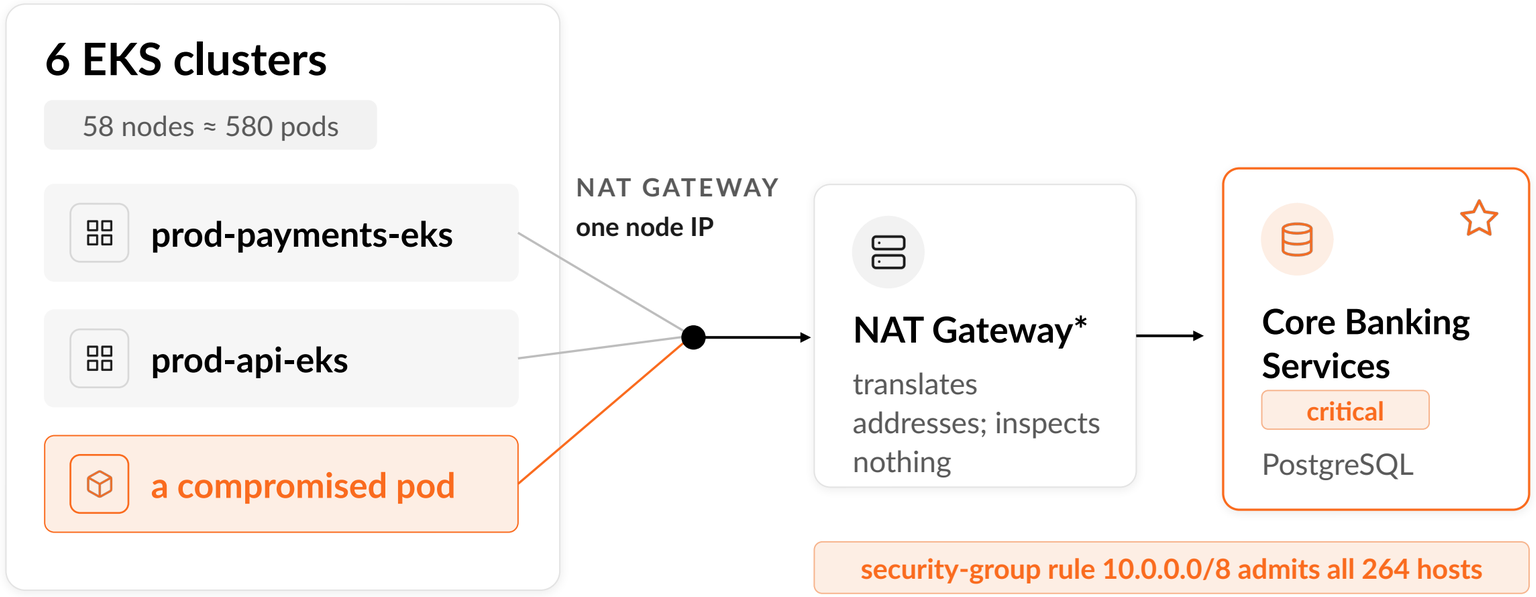
Internal Use Only -

03 · KUBERNETES

Kubernetes nodes are 42% of all footholds

Every pod inherits its node's reach: ~4.8× the 812 hosts (pod estimate).

IN PROD-PLATFORM-VPC, A CRITICAL VPC



One rule admits every pod; the security group can't tell them apart.

* A NAT gateway translates addresses. It doesn't inspect or filter.

EXPOSURE INSIDE CLUSTERS

Footholds into critical systems — 42%
11 internet-facing hosts first, then 341 nodes.

Workloads — 13%
412 of 3,140 workloads.

Blast Radius risk, criticality-weighted — 84%
121 of 146 VPC paths touch a cluster VPC.

Management-port paths — 85%
108 of 127 RDP/SSH paths touch a cluster VPC.

Uninspected internet egress — 19%
260 of 1,334 uninspected workloads.

Paths count per VPC.

THE FIX

Take management ports off the cluster node groups' lateral paths.

Restrict SSH/RDP into node groups to the admin tier; then SmartGroups per namespace and service, policy per pod.

Pods estimated at ~10 per node

Internal Use Only -

04 · SERVERLESS

100% of serverless egress has nothing inspecting it

1,120 serverless workloads, outside every instance count. DCF can group all 1,120 today.

WHAT RUNS

1,120

serverless workloads

AWS Lambda function
940 · 940 in a VPC

Amazon ECS task
164 · 164 in a VPC

Bedrock AgentCore runtime
16 · 16 in a VPC

HOW IT LEAVES



1,120 in 48 VPCs → 62 integration subnets → Internet

Nothing inspects it

1,120

egress uninspected

Integration subnets route to the NAT gateways, not the Aviatrix hubs.

WHAT A SMARTGROUP SELECTS ON

Type, name, region and account: every workload has them. Tags label 31% of them today.

Type
Lambda function · ECS task · AgentCore runtime

Name
prefix match, e.g. payments-*

Region and account
all 1,120 carry both

Tags
347 tagged; the rest need a naming rule

THE FIX

Controller 9.0, then serverless SmartGroups by type and name; DCF egress per SmartGroup.

Point the integration subnets at the Aviatrix hubs, where DCF already runs. Monitor first, then enforce.

DCF for serverless: Controller 9.0, early access

Internal Use Only -

THE WORKSTREAMS

Five workstreams, run in parallel

All start now. Every policy runs in monitor mode first.

1,640
workloads on Aviatrix hubs

154
workloads exposed

38
EKS clusters

1,120
serverless workloads

127
management-port paths

EGRESS	EXPOSURE	KUBERNETES	SERVERLESS	BLAST RADIUS
DCF threat monitoring, hubs first	**Close direct internet exposure**	**Onboard the clusters, production first**	**Serverless SmartGroups, then egress policy**	**One mgmt-port policy between SmartGroups**
Detections name the workload; no routing change on the hubs. Densest NAT VPCs follow.	PSF + DCF for 154 public-IP workloads. Admin ports on 11 hosts first.	SmartGroups per namespace and service; policy per pod.	By type and name; DCF egress per SmartGroup.	Core Banking Services first. −44.6% pivot potential.
policy change	rule change + PSF Gateways	onboarding	controller upgrade + policy	policy design
monitor, then enforce		monitor, then enforce	monitor, then enforce	monitor, then enforce

HAND-OFFS

- Egress → Kubernetes: egress policy for 412 nodes follows the hub gateways.
- Kubernetes → Blast Radius: once onboarded, the management-port policy goes per pod.

Internal Use Only -

PATH TO MONITOR MODE

Half the egress already crosses Aviatrix. Start there

1,640 workloads leave through Aviatrix FQDN hubs, so DCF can see them without re-architecture.

THE EGRESS CHECK

EGRESS THROUGH AVIATRIX?

PARTLY

Yes for 1,640 workloads on the hubs.
Not yet for the 1,334 on NAT and public IPs.

PRE-CHECKS WITH YOUR SE

Licensing: confirm DCF is covered.

Sizing: confirm DCF headroom on the hubs.

Domain lists: export them for WebGroups.

1 DCF on the hubs, nothing enforced
Non-production hubs first; watch what would be blocked.

2 Starter policies
WebGroups carry today's domain lists, plus threat feeds.

3 Review together
What's good, what's bad, likely exfiltration paths in the logs.

4 Workshop for the NAT VPCs
Two hours: plan the first gateways and the route moves.

5 Enforce when ready
Policy by policy, with explicit clearance first.

ROLLBACK, AT ANY STEP

- Monitor mode blocks nothing.
- The FQDN rules stay in place until DCF takes over. Switch back at any time.
- For a NAT VPC, point the route back to the NAT gateway.

Production route changes are planned with Aviatrix Professional Services.

WHAT MONITOR MODE SHOWS

Traffic by domain
Every destination, per workload

Workload names in logs
VM, VPC, account, cluster

Threat and geo detection
Known-bad destinations flagged

What would be blocked
Before any policy is enforced

The gateways also produce DCF logs, which add observed traffic to the next assessment.

Starter policies are SE-applied from one best-practice set. Final set to be confirmed by product.

Internal Use Only -

METHOD AND COVERAGE

What this assessment saw, and what it couldn't

Controller snapshot · read-only, nothing installed, production untouched.

COVERAGE

Inventory and egress paths	Seen	Every workload, traced per subnet route.
Security groups	Seen	1,262 groups; 83% allow outbound to any destination.
East-west reachability	Inferred	From routing and security groups. Not observed traffic.
Kubernetes	Seen	Clusters and nodes. Pods estimated at ~10 per node.
Serverless	Seen	Functions, container tasks and agent runtimes, in and out of VPCs.
AI agents	Inferred	From network interfaces with no instance behind them.
Observed traffic	Not in scope	Add DNS and flow logs to see it.
FQDN domain lists	Not reviewed	Hub paths shown; the lists weren't audited.

HOW THE NUMBERS WERE PRODUCED

- **Containment Graph.** Every workload evaluated against cloud routing, security groups and the controller's gateway, FQDN and NAT configuration.
- **Criticality.** AI-inferred from the inventory. Confirm with your teams.
- **Pivot potential.** The share of VPC-to-VPC management-port paths a policy removes, weighted by the criticality of what they reach.
- **Projections.** The same routing and security-group data, re-evaluated with each workstream applied. Not a measurement.
- **Your data.** A read-only copy of the controller's inventory database and its log bundle, used only for this assessment.

Next layer: add DNS and flow logs to see which east-west paths carry traffic, or turn on monitor mode to add DCF logs.

Sample report. Harborline Financial Group is fictional. Findings are representative of recent assessments; all figures are illustrative.

Internal Use Only -