

THE CASE FOR SOVEREIGN DEFENCE IN MARITIME & LOGISTICS

Keep the cargo moving. Keep *control* from ship to shore.

HiveStørm defends the vessels, terminals and logistics networks your supply chain runs on, against the threats of today and the quantum era, and keeps protecting a vessel even when its link drops, entirely under your control.

● 01 WHY WE DO THIS

A stalled supply chain *stalls the economy.*

Maritime and logistics move the world's goods, and the supply chains they run are critical national infrastructure. A successful attack has already shut down a global shipping line and the ports it touched — costing hundreds of millions and stalling supply chains for weeks. It can misroute a vessel, falsify a manifest, or take a terminal offline. That is a board-level risk, and the threat behind it has changed.

The estate spans vessels at sea and the logistics chain ashore, on intermittently-connected networks. Adversaries are now nation-states and ransomware crews moving at machine speed. The quantum era will break the encryption protecting routing, manifests and navigation. And most security tools depend on foreign clouds — a dependency that, for the supply chain, is itself the vulnerability.

We exist to make the systems an economy can't afford to lose defensible in real time — sovereign, autonomous, and quantum-ready — under their owner's control.

● 02 HOW WE DO IT

One platform. *Not a stack of tools.*

Most organisations bolt together a dozen products from a dozen vendors and staff a team around the clock to watch them. HiveStørm is one engine that does three fused jobs — it understands everything your systems do, detects and stops threats on its own, and protects your data against today's and tomorrow's code-breakers — and it runs entirely inside your walls. Three things make it different, and all three are business advantages, not features:

Sovereign

It runs on your infrastructure, in your jurisdiction, with no foreign dependency. You own it outright; nothing leaves your estate, and nothing relies on a service you don't control.

Autonomous

It contains threats in seconds, and keeps protecting a vessel even when its satellite link drops. Your protection doesn't depend on a team noticing and reacting in time.

Quantum-ready now

It protects your data and control links with quantum-safe encryption today — not as a future migration project — closing a gap your competitors are still scoping.

The effect is one platform a leaner team can run, defending your most critical systems at machine speed, proving every decision it makes, and keeping you firmly in control.

03 WHAT IT LOOKS LIKE IN PRACTICE

A shipping line, *under quiet attack*.

ILLUSTRATIVE SCENARIO

A logistics operator runs a fleet and the terminals that serve it. *A ransomware crew slips in through the shore-side network and moves toward vessels and terminal operations.*

THE SITUATION	Shore-side IT, terminal systems and vessel networks are interconnected across the chain. The attacker gains a foothold and begins moving toward cargo and terminal operations.
WITHOUT MODERN DEFENCE	Each step looks like ordinary traffic. By the time it surfaces, the attacker can halt a terminal, misroute a vessel or falsify manifests — and harvested data can be unlocked later, once quantum computers arrive.
WITH HIVESTORM	The platform has learned the chain's normal rhythm. It recognises the attack as one connected event , isolates the compromised systems in seconds — and keeps protecting a vessel even with its link down — re-keying with quantum-safe encryption. Every action is sealed into a tamper-evident record.
THE OUTCOME	Cargo keeps moving. The attack is contained before it disrupts operations, the operator can prove what happened, and harvested data is worthless — today and in the quantum era.

THE BUSINESS VALUE

What each leader gets.

FOR THE CEO

- Continuity of supply and reputation protected from a port or fleet incident.
- A supply-chain disruption avoided — resilience you can speak to with confidence.
- A clear, sovereign answer for customers and the board.

FOR THE CIO & CISO

- One sovereign platform across fleet and shore, working even on intermittent links.
- Far less load on a stretched team — the platform acts on its own.
- Audit-ready by design, with quantum migration handled rather than deferred.

FOR THE Board & Risk

- A demonstrable, defensible security posture.
- Reduced regulatory, insurance and liability exposure.
- Resilience that protects the supply chain and enterprise value.

WHY NOW

The clock is already running. Standards bodies require moving off today's encryption between 2030 and 2035, the estimates for when quantum computers can break it keep accelerating, and "harvest now, decrypt later" means data taken today is already at risk. Shipboard and terminal systems carry long lifecycles and slow replacement cycles — so starting now is not early. It is the only way to be ready in time.

NEXT STEP

STEP 01

Demo

See the platform defend a vessel-and-terminal environment.

STEP 02

Exposure report

A passive, no-obligation assessment of where your estate is exposed — nothing installed.

STEP 03

Bounded proof of concept

A scoped trial in one part of your environment, with success measures agreed up front.