THE CASE FOR SOVEREIGN DEFENCE IN DEFENCE & AEROSPACE

Win the mission. Keep *command* of the systems that deliver it.

HiveStørm defends mission systems, command networks and autonomous platforms — air-gapped, on-premise and entirely sovereign — against the threats of today and the quantum era, with no foreign disclosure.

01 WHY WE DO THIS

A compromised system *is a compromised mission.*

For defence and aerospace, a successful intrusion is not a data-breach headline — it can corrupt a mission system, spoof a command, ground a fleet, or hand an adversary the decision advantage. The threat is a state-level adversary with state-level patience, and commercial tooling built for a different threat model cannot answer it.

Mission systems, weapons and autonomous platforms now act at machine speed, and the adversary aims at the gap where the operator is squeezed out of the decision. The quantum era will break the encryption protecting classified traffic and command channels — and harvested data has a shelf life measured in decades. Most security tools depend on foreign clouds and services, an unacceptable dependency for sovereign capability.

> *We exist to make the systems a nation can't afford to lose defensible in real time — sovereign, autonomous within doctrine, and quantum-ready — under its own command.*

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 air-gapped and on-premise by default, in your jurisdiction, with no foreign disclosure. You hold it outright; nothing leaves, and nothing depends on a foreign service.

Autonomous

It contains threats at machine speed within doctrine — operator-in-the-loop where your rules require. Fast enough for the fight, never beyond what you authorise.

Quantum-ready now

It protects classified traffic and command channels with quantum-safe encryption today — not as a future migration — against data harvested now and decrypted later.

The effect is one platform that defends from the data centre to the forward edge, acts within doctrine, proves every decision, and stays entirely under your command.

03 WHAT IT LOOKS LIKE IN PRACTICE

A mission network, *under state attack.*

ILLUSTRATIVE SCENARIO

A defence operator runs mission systems and command nodes, some air-gapped at the forward edge. *A state-level group attempts to penetrate the network and forge command traffic.*

THE SITUATION	The adversary probes the mission network patiently, looking to move toward command-and-control and impersonate an authorised operator.
WITHOUT MODERN DEFENCE	Each move blends into normal operations. By the time analysts react, the adversary may be positioned to spoof commands or exfiltrate classified data — data that can be unlocked later, once quantum computers arrive.
WITH HIVESTØRM	The platform recognises the intrusion as **one connected attack**, **contains it within doctrine in seconds**, and ensures command channels accept only cryptographically authenticated, quantum-safe instructions. Every action is sealed into a tamper-evident record — fully sovereign, no foreign disclosure.
THE OUTCOME	**The mission holds.** The intrusion is contained before it reaches command, autonomous platforms stay within authorised limits, and harvested data is worthless — today and in the quantum era.

THE BUSINESS VALUE

What each leader gets.

FOR

Programme leadership

- Mission continuity and decision advantage protected.
- Sovereign capability with no foreign dependency or disclosure.
- A credible answer on resilience to the customer and the chain of command.

FOR

CISO & security

- One sovereign platform from data centre to forward edge.
- Autonomous response within doctrine, operator-in-the-loop where required.
- Audit-ready by design, with quantum migration handled rather than deferred.

FOR

Mission assurance & risk

- A demonstrable, defensible posture — every machine decision recorded.
- Reduced disclosure and supply-chain exposure.
- Provable assurance that platforms stay within authorised limits.

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. Defence systems carry the longest lifecycles of all, and the most sensitive long-lived data — 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 mission-like 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.