

THE CASE FOR SOVEREIGN DEFENCE IN MANUFACTURING

Keep the line running. Keep *control* of the machines that run it.

HiveStørm defends the plants, robots and control systems your business runs on, against the threats of today and the quantum era. One platform, run entirely under your control, that detects and stops attacks on its own and keeps your production trustworthy in real time.

● 01 WHY WE DO THIS

A stopped line *is a stopped business.*

A successful attack on a manufacturer is not an IT problem with a price tag. It can halt a production line, scrap a batch, damage equipment, threaten worker safety, and stall the supply chains your customers depend on — in minutes. That is a board-level risk, and the threat behind it has changed.

The old model — a wall around the network, watched around the clock by analysts — was built for a slower world. Adversaries are now nation-states and ransomware crews moving at machine speed. The IT network and the operational technology running the plant floor have merged. The quantum era will break the encryption protecting today's control systems. And most security tools depend on foreign clouds — a dependency that, for critical production, is itself the vulnerability.

We exist to make the systems a business 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, within the limits you set — without stopping the line. 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 factory, *under quiet attack*.

ILLUSTRATIVE SCENARIO

A manufacturer runs robots, controllers and historians across a plant where IT and OT merged years ago. *A ransomware crew slips in through a remote-maintenance link.*

THE SITUATION	The plant network and the business IT have grown together. The attacker gains a quiet foothold and begins moving toward the controllers that run the physical line.
WITHOUT MODERN DEFENCE	Each step looks like ordinary activity on its own. By the time an analyst pieces it together, the attacker is ready to halt production or encrypt the controllers — and any data copied can be unlocked later, once quantum computers arrive.
WITH HIVESTORM	The platform has learned each machine's normal rhythm. It recognises the unusual sequence as one connected attack , isolates the compromised segment in seconds without stopping the line , and re-keys the affected links with quantum-safe encryption the moment it senses trouble. Every action is sealed into a tamper-evident record.
THE OUTCOME	The line keeps running. The attack is contained before it reaches the physical process, the operator can prove exactly what happened, and the data the attacker took is worthless — today and in the quantum era.

THE BUSINESS VALUE

What each leader gets.

FOR THE CEO

- Continuity of production and on-time delivery protected from a headline-grade incident.
- A safety, shutdown or product-integrity event avoided.
- A clear, sovereign answer when customers and the board ask “are we resilient?”

FOR THE CIO & CISO

- One sovereign platform across IT and OT, replacing a sprawling toolset of [N] products.
- Far less load on a stretched team — the platform acts on its own within your rules.
- Audit-ready by design, with quantum migration handled rather than deferred.

FOR THE Board & Risk

- A demonstrable, defensible security posture — evidence for every decision.
- Reduced safety, regulatory and liability exposure across the estate.
- Resilience that protects output, delivery 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. Critical manufacturing and operational technology carry some of the longest upgrade cycles of any sector — 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 plant-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.