

THE CASE FOR SOVEREIGN DEFENCE IN FOOD & AGRICULTURE

Keep the food flowing. Keep *control* from field to plant.

HiveStørm defends the farms, machinery and food-production systems your business — and your country — depends 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 operations running, even at a remote site with no connection.

● 01 WHY WE DO THIS

Food security *is national security.*

A successful attack on a food producer is not an IT problem with a price tag. It can halt a harvest, spoil produce, idle a processing line, contaminate a batch, or take the food supply offline — threatening safety and public confidence in hours. 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 who treat the food supply as leverage, moving at machine speed. Corporate IT and the operational technology running farms and plants have merged, much of it on remote sites with little security on hand. The quantum era will break the encryption protecting control systems and the valuable data agritech runs on. And most security tools depend on foreign clouds — a dependency that, for critical food infrastructure, is itself the vulnerability.

We exist to make the systems a nation feeds itself with 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 without stopping the harvest or the processing line, and keeps protecting a remote site even when its connection drops. Defence at the speed of the attack.

Quantum-ready now

It protects your control links, machine identity and agritech data with quantum-safe encryption today — not as a future migration project — so commands can't be forged and data can't be harvested for later.

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 food producer, *under quiet attack*.

ILLUSTRATIVE SCENARIO

A producer runs autonomous machinery, irrigation and sensors across remote farms, feeding a processing plant and cold-chain. *A ransomware crew slips in through a remote-maintenance link.*

THE SITUATION	IT and the operational technology across farms and the plant have grown together, much of it on intermittent links. The attacker gains a quiet foothold and moves toward the systems that run machinery and processing.
WITHOUT MODERN DEFENCE	Each step looks like ordinary activity, and a remote site may be cut off from head-office monitoring. By the time it surfaces, the attacker can halt the harvest, spoil a batch or encrypt control systems — and any data copied can be unlocked later, once quantum computers arrive.
WITH HIVESTORM	The platform runs sovereign at the site and has learned its normal rhythm. It recognises the unusual sequence as one connected attack , isolates the compromised segment in seconds without stopping operations — even with the link to head office down — and re-keys the affected links with quantum-safe encryption. Every action is sealed into a tamper-evident record.
THE OUTCOME	The food keeps moving. The attack is contained before it reaches the physical process, the producer can prove exactly what happened to regulators and buyers, 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 supply and public confidence protected from a headline-grade incident.
- A food-safety or shutdown event avoided — resilience you can speak to with confidence.
- A clear, sovereign answer when buyers, regulators and the board ask “are we resilient?”

FOR THE CIO & CISO

- One sovereign platform across IT, farm OT and the processing plant, replacing a toolset of [N] products.
- Far less load on a stretched team — the platform acts on its own, even on intermittent links.
- 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 food-safety, regulatory and liability exposure across the estate.
- Resilience that protects supply, brand 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. Farm machinery, remote operational technology and food-plant 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 farm-and-plant 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.