THE CASE FOR SOVEREIGN DEFENCE IN PHARMA & BIOTECH

# Protect the discovery. Protect the *integrity* of how it's made.

HiveStørm defends the research data and manufacturing systems your science runs on — the IP that defines your future and the production that reaches patients — against the threats of today and the quantum era, entirely under your control.

01 WHY WE DO THIS

## Your IP is the company. *Your production is patient safety.*

Pharma and biotech run on secrets and on safety. A successful attack can exfiltrate the formulations and trial data that represent a multi-billion-dollar lead, or tamper with the manufacturing that reaches patients. Either is a board-level event, and the threat behind it — nation-state and competitor espionage moving at machine speed — has changed.

Two estates are under attack at once: the research IT where the IP lives, and the regulated manufacturing floor where a compromise threatens patient safety. The quantum era will break the encryption protecting IP and trial data — harvested today, decrypted later. And most security tools depend on foreign clouds, a dependency that, for irreplaceable science, is itself the exposure.

> *We exist to make the assets a company can't afford to lose defensible in real time — sovereign, autonomous, and quantum-ready — under its own 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 — before IP leaves the building or a batch is touched. Your protection doesn't depend on a team noticing and reacting in time.

### Quantum-ready now

It protects IP and trial data with quantum-safe encryption today — not as a future migration project — against data harvested now and decrypted 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 research estate, *quietly raided.*

ILLUSTRATIVE SCENARIO

A biotech runs research IT alongside a regulated manufacturing floor. *A nation-state group targets the formulation and trial data behind a lead programme.*

| | |
|---|---|
| THE SITUATION | The attacker gains a quiet foothold in the research network and begins locating and staging the IP — formulations, genomic datasets, trial results — for exfiltration. |
| WITHOUT MODERN DEFENCE | The activity resembles normal research access. By the time it surfaces, a decade of R&D may already be gone — and any encrypted data taken can be unlocked later, once quantum computers arrive. |
| WITH HIVESTØRM | The platform has learned where the IP lives and how it's normally used. It flags the exfiltration as **one connected attack**, **contains it in seconds before the data leaves**, and protects every link with quantum-safe encryption. Every action is sealed into a tamper-evident record. |
| THE OUTCOME | **The IP stays in-house.** The exfiltration is stopped before it completes, manufacturing integrity is preserved, the company can prove what happened, and any data taken is worthless — today and in the quantum era. |

THE BUSINESS VALUE

## What each leader gets.

FOR THE

### CEO

- Irreplaceable IP and research lead protected.
- A patient-safety or production-integrity incident avoided.
- A clear answer on resilience for partners, regulators and the board.

FOR THE

### CIO & CISO

- One sovereign platform across research IT and the manufacturing floor.
- 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 posture and provable data integrity.
- Reduced regulatory and liability exposure.
- Protection of the pipeline that is 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. Regulated manufacturing and long-lived research data carry long upgrade 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 research-and-production 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.