

THE CASE FOR SOVEREIGN DEFENCE IN FINANCE

Keep the markets moving. Keep *proof* of every move you make.

HiveStørm defends the trading and settlement infrastructure your institution runs on, at market speed, against the threats of today and the quantum era — and proves the integrity of every transaction, entirely under your control.

● 01 WHY WE DO THIS

In finance, *trust is the product.*

Banking and capital markets are critical national infrastructure, and a successful attack is measured in more than losses. It can halt settlement, undermine the integrity of transactions, trigger regulatory action, and erode the trust an institution is built on — at machine speed. That is a board-level risk, and the threat behind it has changed.

The old model — perimeter defence watched by analysts, batch checks at end of day — was built for a slower world. Adversaries now move faster than any review cycle. The quantum era will break the encryption protecting settlement, identity and transaction integrity. And most security tools depend on foreign clouds — a dependency that, for financial infrastructure, is itself the vulnerability.

We exist to make the systems a market 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 at market throughput — catching insider and takeover activity as it happens, not in an end-of-day batch. Defence at the speed of the attack.

Quantum-ready now

It protects settlement and transaction data with quantum-safe encryption today — not as a future migration project — and proves integrity rather than just claiming it.

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 settlement rail, *under quiet attack*.

ILLUSTRATIVE SCENARIO

An institution runs trading and settlement systems at market throughput. *An insider, with valid credentials, begins manipulating transactions ahead of an end-of-day check.*

THE SITUATION	The institution processes enormous transaction volumes in real time. An insider with legitimate access starts subtly altering instructions, betting the activity won't surface until the end-of-day batch.
WITHOUT MODERN DEFENCE	Each action looks authorised on its own. A batch review might catch it hours later, after settlement — and any encrypted financial data harvested can be unlocked later, once quantum computers arrive.
WITH HIVESTORM	The platform has learned normal transaction behaviour. It flags the manipulation as it happens, not end-of-day , contains it in seconds, and seals every instruction with quantum-safe signing so integrity is provable . Every action is recorded in a tamper-evident log.
THE OUTCOME	The manipulation is caught at event speed. Settlement integrity holds, the institution can prove exactly what happened to a regulator, and harvested data is worthless — today and in the quantum era.

THE BUSINESS VALUE

What each leader gets.

FOR THE CEO

- Trust and reputation protected from a settlement or integrity incident.
- A market-facing crisis avoided — resilience you can speak to with confidence.
- A clear, sovereign answer for regulators, clients and the board.

FOR THE CIO & CISO

- One sovereign platform at market throughput, replacing a toolset of [N] products.
- Insider, takeover and manipulation detection in real time, not at end of day.
- Audit-ready by design, with quantum migration handled rather than deferred.

FOR THE Board & Risk

- A demonstrable, defensible and provable security posture.
- Reduced regulatory and liability exposure across the estate.
- Integrity that protects enterprise value and licence to operate.

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. Financial infrastructure holds long-lived, sensitive data and faces tightening expectations — 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 settlement-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.