HIVESTØRM

STORM PLATFORM

PRIVATE WEALTH & FAMILY OFFICES / SECTOR

PRODUCT DATASHEET

STATE-GRADE DEFENCE · CUSTODY · IDENTITY · CONTINUITY · NO SECURITY TEAM REQUIRED

THE PROBLEM

Family offices and private institutions are high-value targets defended by small teams. The adversaries are the same state-grade actors that target banks and governments — but the defences are private-sector, and often thinly staffed.

Custody, settlement, identity and audit are exposed to the same AI-driven tradecraft and quantum decay that targets sovereign systems. Attackers personalise the approach and move at machine speed, and an alert queue waiting for an analyst is no defence at all.

And encrypted data — wire instructions, identity records, holdings — harvested today can be decrypted later. Discretion lost once is lost permanently.

THE SOLUTION

HiveStørm gives a small team sovereign-grade defence that runs itself. It learns what normal looks like across your systems, recognises what doesn't belong, and contains it autonomously — no security operations centre, no analyst in the loop.

It protects custody, settlement and identity with post-quantum cryptography, keeps your data in your chosen jurisdiction, and seals every action into a tamper-evident record. Quiet, sovereign, always on.

> *Sovereign-grade defence, sized for the team you actually have.*

01 KEY BENEFITS

- State-grade defence without a security team to run it.
- Threats contained automatically — no alert queue, no analyst on call.
- Custody, settlement and identity protected against the quantum threat.
- Understands the sequence, not just the alert.
- Discretion by design — nothing leaves your estate.
- A tamper-evident record for auditors, banks and trustees.

02 FEATURE SPOTLIGHT

Runs without a security team

Autonomous response means no queue and no night shift.

Protects what matters most

Custody, identity and settlement — not just the network.

Learns your normal

Flags activity that doesn't belong, even when it's never been seen before.

Quantum-safe from day one

Protects sensitive records against "harvest now, decrypt later".

DEPLOYMENT

Sovereign cloud, hybrid, or fully managed — protection without the operational headcount.

COMPLIANCE & ASSURANCE

Data residency and jurisdictional control by design; supports privacy and fiduciary obligations.

WHAT IT IS

Two defences fused into one sovereign platform.

HiveStørm is a **Sovereign XDR** that detects and contains the threat, and a **post-quantum cryptographic layer** that protects your data as it moves. One platform does both — and it runs without a security team. Both run on one stateful event intelligence engine — it remembers what came before, so it sees patterns, not isolated events.

PILLAR A

SOVEREIGN XDR

DETECT & CONTAIN

- Watches every system across the office, learns what normal looks like, and contains what doesn't belong — autonomously, in seconds, with no analyst in the loop.
- **Sovereign** means it runs in your jurisdiction, under your control — nothing leaves, nothing depends on a foreign service.
- Extended detection and response that protects a small team without expanding it.

PILLAR B

POST-QUANTUM DEFENCE

PROTECT DATA IN TRANSIT

- Wire instructions, identity records and holdings data are encrypted with post-quantum key exchange — so anything harvested today can't be read later when quantum computers arrive.
- Custody, settlement and identity channels are cryptographically bound and sealed, so a transaction can be trusted and proven after the fact.
- Quantum-safe from day one — no migration project, no specialist team required.

ONE LOOP, NOT TWO PRODUCTS DETECT ⇄ RE-KEY

Detection and cryptography aren't two bolted-together products — they work as one loop. When the XDR layer detects a compromise indicator, it triggers the cryptographic layer to re-key the affected channels in seconds. The defence reacts the moment something is wrong.

> *Most vendors sell detection or post-quantum cryptography. HiveStørm fuses them — and runs them for you.*

04 WHAT THIS MEANS FOR THE FAMILY OFFICE

- **State-grade protection without a state-grade team.**
- **Custody and identity stay private — today and against tomorrow's quantum threat.**
- **Detection and encryption work as one system you don't have to operate.**
- **A sovereign, auditable record for banks, auditors and trustees.**

UNDER THE HOOD

A stateful event intelligence engine ingests from any source and keeps the memory of what came before. Built on NIST-standardised post-quantum algorithms (`ML-KEM`, `ML-DSA`) with zero foreign dependencies — sovereign, and standards-based.

05 NEXT STEP

STEP 01
DEMO
Guided Storm Platform demonstration

→

STEP 02
EXPOSURE REPORT
Storm Rune cryptographic exposure report

→

STEP 03
BOUNDED POC
Scoped proof-of-concept, your environment