

THE CASE FOR SOVEREIGN DEFENCE IN MINING & METALS

Keep production flowing. Keep *control* of the sites that deliver it.

HiveStørm defends the remote sites, processing plants and control systems your operation runs on — pit to refinery — against the threats of today and the quantum era, and keeps protecting even when a site's link drops, entirely under your control.

● 01 WHY WE DO THIS

A halted mine *is millions a day*.

Mining and metals supply the strategic resources the world runs on, and a successful attack costs millions a day and can ripple through a national supply chain. It can stop production, threaten worker safety — hoists, ventilation, tailings — or take a remote site offline. That is a board-level risk, and the threat behind it has changed.

The estate spans remote pits, processing plants and refineries where IT and operational technology merged long ago, often on intermittent satellite links. Adversaries are now nation-states and ransomware crews moving at machine speed. The quantum era will break the encryption protecting control systems and metallurgical IP. And most security tools depend on foreign clouds — a dependency that, for strategic resources, is itself the vulnerability.

We exist to make the systems an operation 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 without halting production, and keeps working even when a remote site's link to head office drops. Defence at the speed of the attack.

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 remote site, *under quiet attack*.

ILLUSTRATIVE SCENARIO

A miner runs autonomous haulage, processing circuits and smelters across remote sites on satellite links. *A ransomware crew slips in through a contractor's remote access.*

THE SITUATION	IT and the site OT have grown together across remote, intermittently-connected locations. The attacker gains a foothold and moves toward the systems controlling processing and haulage.
WITHOUT MODERN DEFENCE	Each step looks routine, and a remote site may be cut off from head-office monitoring. By the time it surfaces, the attacker can halt production or encrypt control systems — and harvested data 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 attack as one connected event, isolates the compromised segment in seconds without halting production — even with the link to head office down — and re-keys with quantum-safe encryption. Every action is sealed into a tamper-evident record.
THE OUTCOME	Production keeps flowing. The attack is contained before it reaches the physical process, the operator can prove what happened, and harvested data is worthless — today and in the quantum era.

THE BUSINESS VALUE

What each leader gets.

FOR THE CEO

- Continuity of production and output protected from a costly incident.
- A safety or shutdown event avoided.
- A clear, sovereign answer when the board asks "are we resilient?"

FOR THE CIO & CISO

- One sovereign platform across IT and site OT, working even on intermittent links.
- 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 security posture.
- Reduced safety, regulatory and liability exposure.
- Resilience that protects output 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. Remote operational technology and long-lived industrial assets 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 site-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.