IBLADES WHITEPAPER · PORTS & MARITIME

Quantum-Safe Ports & Maritime Logistics

Isolating crane and terminal automation, protecting high-value trade data, and securing vessels — overlaid on existing port and shipping infrastructure without downtime.

← Aerospace & Transportation

In this paper

1. Executive summary

Modern ports are hyper-automated logistics platforms: robotic cranes, automated storage, digital trade documents, and IoT sensor meshes. That automation creates a dual risk — kinetic cyberattacks that can paralyze terminal operations, and the harvesting of high-value trade-finance data for future quantum decryption.

iBlades secures maritime logistics with a hardware-anchored, post-quantum fabric that overlays existing infrastructure. It isolates operational technology from IT and the public internet, protects digital trade documents and vessel communications, and counters AI-driven attacks by shrinking the exposed software surface — with no operational downtime.

2. The 2026 threat landscape

Kinetic attacks on port automation

Ransomware and logic bombs targeting crane, stacker, and automated-storage controllers can halt a terminal and cost millions per hour. These programmable controllers were rarely designed for internet exposure and cannot easily be patched.

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing exposed services, generating evasive malware, and moving laterally after a foothold. **Data poisoning** of sensor feeds can corrupt the port "digital twin," driving wrong operational decisions.

> **The real target is complexity.** AI attacks feed on exposed interfaces, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Harvest Now, Decrypt Later (HNDL)

Bills of lading, trade-finance documents, and supply-chain manifests intercepted today can be decrypted once quantum computers mature — exposing commercially sensitive data with a long shelf life.

---

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM and ML-DSA/Dilithium; FIPS 203/204) with keys generated locally and rotated autonomously.

- **GuardTron™** — hardware "red zone" isolating crane, stacker, and PLC control systems from IT and the public internet; also deployable on vessels to encrypt satellite links and protect navigation systems.
- **NetTron™** — software-defined, peer-to-peer quantum-safe mesh; applies post-quantum encryption to electronic bills of lading and trade documents, and

authenticates the sensor data feeding the digital twin.

- **ManoTron™** — hardware-secured mobile communications and leak-proof asset tracking for security patrols and field teams.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement from IT into port OT.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, EDR/XDR, SASE, and identity tools.

---

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across the fabric
IMO MSC.428(98)	Maritime cyber risk management	Vessel link encryption, navigation-system protection
ISO 28000	Supply-chain security management	Trade-document PQC, OT red-zone isolation
IEC 62443	Industrial / OT security	Hardware segmentation for crane and terminal controllers
ISO 27001	Information security management	Zero-trust access, immutable audit trails

---

5. A low-risk pilot path

- **Select** one automated asset or control link (e.g., a storage block or a single crane set).
- **Deploy** the edge node inline to isolate the controllers — no changes to the automation system.
- **Validate** with a lateral-movement simulation; legitimate commands pass, unauthorized access is blocked.
- **Demonstrate** post-quantum key rotation and audit evidence; reverse cleanly if desired.

Ready to secure your port operations?

Request a briefing to see how a low-risk pilot would work in your environment.

Request a briefing

⬇ Download PDF

Back to overview

Prefer email? Reach us at hello@iblades.ai

Safe, effective, secure.

Next-generation cyber architecture making cybersecurity simple, reliable, and accessible for everyone.

hello@iblades.ai

Products

- NetTron™
- GuardTron™
- ManoTron™
- Pricing

Solutions

- Financial Institutions
- Healthcare
- Infrastructure
- Government & Military

Company

- About Us
- Partners
- Documentation
- Contact

Compliance

- NIST Approved
- SOC 2 Type II
- HIPAA Compliant
- ISO 27001
- FedRAMP Ready

HEADQUARTERS
127 Spring Street, Suite 120
Pleasanton, CA 94566

R&D CENTER
795 24th Street
Ogden, UT 84401