KerioControl

USE CASE

When Starlink isn’t enough

Fleet network management and security for the connected vessel

The problem no one planned for



Starlink solved maritime bandwidth. It didn't solve what comes after.

Vessels now run 200–600 Mbps at sea. The moment the crew discovered real internet access, they used it: streaming, gaming, cloud sync. On a flat network with no traffic management, that consumption fills whatever Starlink delivers. Navigation systems, ECDIS displays, and shore VPN tunnels now compete against unlimited recreational demand on the same pipe.

More bandwidth without management produces worse outcomes for the systems that matter most.

There's a second problem bandwidth can't fix: a flat vessel network gives a compromised crew device a direct path to navigation equipment and the shore command center. Marlink's 2025 data found 82% of maritime security alerts originated in crew zones. IMO Resolution MSC.428(98) has required documented cyber risk management across all vessels since January 2021. Most operators know the requirement. Fewer have the controls to prove it.

What GFI KerioControl does

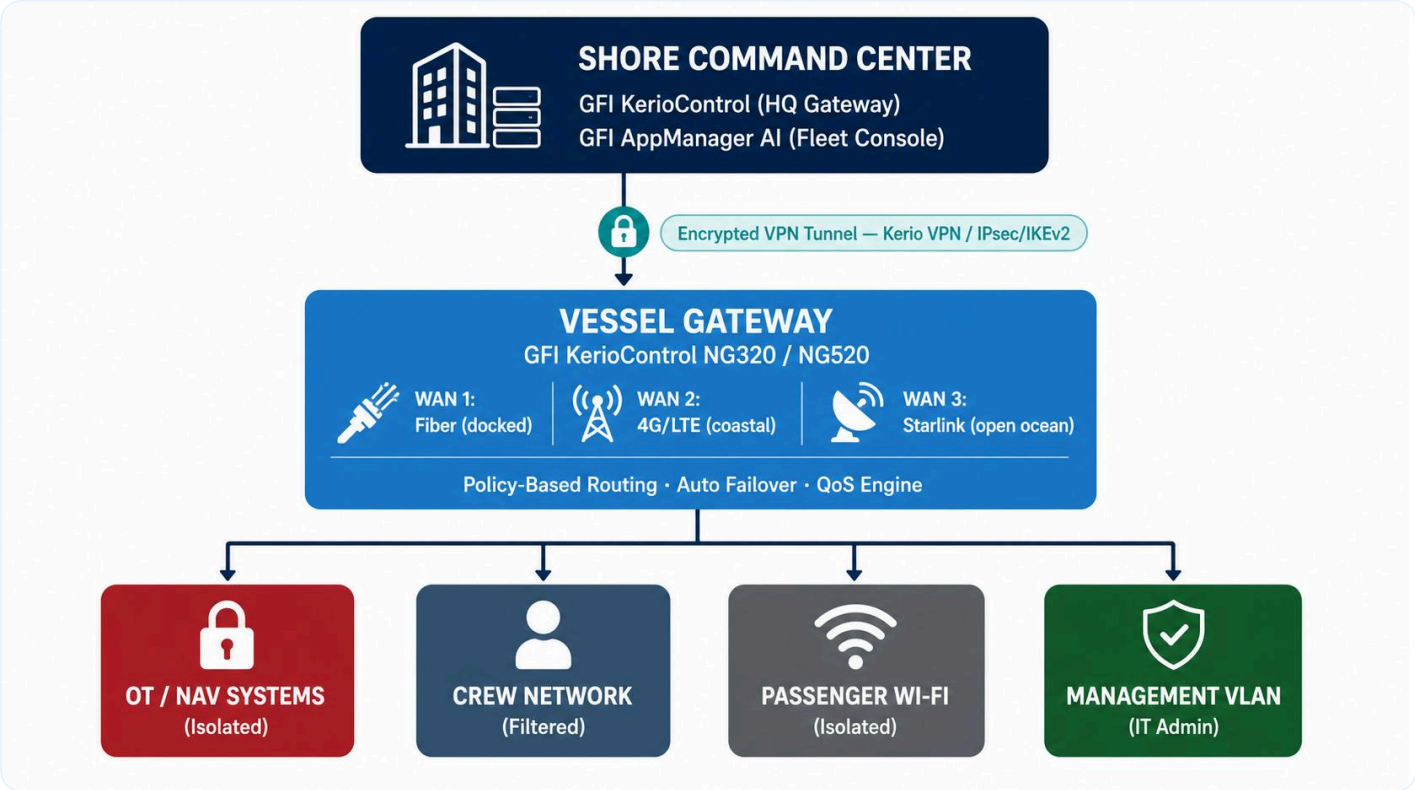
Two problems. One appliance.

GFI KerioControl manages which traffic gets priority across every WAN link, so navigation systems always win regardless of crew demand. It also enforces hard zone isolation between every onboard network segment, so a compromised crew device has nowhere to go.

A GFI KerioControl appliance (NG120, NG320, NG520/NG521, or NG720) terminates all WAN connections at the vessel's perimeter and enforces policy between every onboard segment. Every physical port on the appliance is fully configurable, with any port able to serve as a WAN or LAN interface and no fixed assignments. That means a single NG521 can manage up to 7 simultaneous WAN connections, and the NG720 up to 15, always reserving at least one port for the internal vessel network. Fiber at port, 4G near shore, and Starlink at sea can all run simultaneously on one box. An encrypted VPN tunnel connects each vessel to the shore command center, where GFI AppManager AI gives the IT team a live view of the entire fleet from one console.

Three links, one intelligent gateway

A vessel transitions constantly between connectivity types. GFI KerioControl manages the handoffs automatically.



Link	When used	Policy
Fiber (port)	Bulk transfers, updates, downloads	Unrestricted
4G/LTE (coastal)	Standard near-shore operations	Per-zone QoS
Starlink (open ocean)	Primary at sea	OT guaranteed first

When a link fails, traffic moves to the next available connection in under 60 seconds, with no dropped VPN sessions, no crew intervention. Large software updates scheduled to fiber at port and are suppressed on Starlink. Navigation data always has a reserved path.

Priority where it matters

Navigation and OT systems receive the highest QoS class: guaranteed throughput, never throttled, regardless of what the crew is consuming. Shore VPN sits in a reserved pool. Crew entertainment is rate-managed per user. Automated backups are suppressed at sea entirely.

The result: ECDIS and AIS receive consistent performance even when every crew member is streaming at full Starlink speed.

Segmentation: Containing the breach

Maritime network incidents doubled in 2025. The pattern is consistent: a compromised crew device reaches everything on a flat network.

GFI KerioControl applies default **DENY ALL** between every vessel zone. Nothing crosses a boundary without an explicit rule mapped to a named AD user.

Zone	Default policy
OT / Navigation	Fully isolated. Shore VPN via explicit rule only.
Crew Corporate	Internet via content filter. No OT access.
Passenger / Guest Wi-Fi	Rate-limited internet only. Fully isolated.
Management VLAN	2FA-authenticated. IT admin only.

A compromised crew device stays in the crew zone and cannot reach the bridge, engine monitoring, or shore infrastructure.

Fleet visibility from shore

GFI AppManager AI turns Starlink's always-on connection into continuous fleet oversight:

- One dashboard for WAN status, VPN health, bandwidth, and security events across every vessel
- Policy templates — write once, push to the entire fleet simultaneously
- ClearView — per-user, per-application visibility where Starlink shows only aggregate data

Two IT administrators. Twelve vessels. One console.

GFI KerioControl vs Starlink alone

What matters	GFI KerioControl	Starlink alone
Per-zone / per-user QoS	✅ Granular, policy-based	❌ Not available
OT / crew / guest isolation	✅ Default DENY ALL zones	❌ Not a security product
Multi-WAN failover	✅ Automatic, <60 sec	❌ Single-link only
Fleet management console	✅ GFI AppManager AI	❌ Per-vessel only
IMO compliance documentation	✅ Logs + one-click reports	❌ Aggregate data only

Ready to get started?

Talk to GFI at sales@gfi.com or find a partner.

Copyright © GFI USA, LLC, All rights reserved.