

SHIPGUARD™

Information Technology (IT) services (servers, laptops, desktops PCs) are increasingly connected to the same infrastructure as Operational Technology (OT) systems which manage the operating and safety functions of a vessel.

This interconnectivity provides a much better integrated user experience, but unfortunately brings with it the risks of cross-pollution of malware, viruses and ransomware.


SHIPGUARD™ is an integrated network cyber security system that allows IT and OT systems on a vessel to share resources and interact with each other safely.


SHIPGUARD™ also protects legacy equipment in an OT network where software patching is no longer viable.


CONTACT OUR TEAM TO DISCUSS


PROTECTING IT AND OT CONNECTED NETWORKS AND LEGACY EQUIPMENT ON SHIPS


SHIPGUARD™ FUNCTIONALITY


- 


Small, lightweight, and low power consumption platform combining firewall, gateway anti-virus, intrusion detection and a range of additional protection layers and complex service capabilities
- 

Network Firewall filtering by source and destination IP & Geography destination, content and data rate
- 

Provides granular control over source (IP address and geography), destination, content and data rate
- 


Allows IT functions (email, web Browsing, etc) to operate safely without risk to the vital OT systems
- 


Controlled access for OT systems to both IT systems and the internet for updating /patching of systems and remote support
- 


All actions are logged, permitting anomaly or forensic analysis
- 


The ShipGuard™ platform may be used as secure host for multiple layers of 3rd party extra function software


SHIPGUARD™ KEY FEATURES


- 


Router preventing malware propagation
- 


Gateway Antivirus for traffic between networks and inbound from the internet
- 

Multiple VPN options – server or client
- 

Management of time-limited access
- 

Intrusion Detection System (IDS) – monitors the networks or systems for malicious activity or policy violations
- 

NTP Server – applies consistent time to enable reading of multiple logs
- 

Bandwidth control to guarantee Internet availability and Quality of Service (QoS)
- 

Web Proxying with content filtering - reduces bandwidth consumption

 MONTHLY SUBSCRIPTION OPTION