

CYBERGUARD:

Safeguarding your business in the Digital Age

MARLINK
ABOVE AND BEYOND

Sophisticated cyber security solutions to support your vessel digitalisation

Broadband connectivity at sea and the increasing use of digital systems for everything from navigation to container inspection has led to reduced operational cost and improved efficiency in the shipping industry, but it has also created a new type of threat – cyber risk. While increasing communication provisions have enabled seafarers to use an average of three devices onboard, insecure private devices may provide a vulnerability in the vessel's IT system.

Whether in regard to the protection of data, potential damage and loss, liability, compliance, or the impact on insurance, companies need to be aware and well covered as they seek to balance digital opportunity with new cyber threats.

A holistic approach to security is needed that enables response to new and ever-evolving risks. To support your IMO2021 compliance and help protect you from potential business disruption caused by a cyber attack, Marlink's CyberGuard security portfolio supports your business' digitalisation and enables you to focus on your core business.

CyberGuard Solutions Portfolio - Our Framework

Marlink's vision is an automated and standardised architecture converging IT and Operational Technology (OT). Our communication experts are eager to understand your requirements and consult on the ideal blend of services.

Protecting a Maritime IT & OT network against cyber threats requires a combination of proven tools and processes. This avoids you being in a position of having to pay hackers a ransom, pay a fine to national bodies or suffering from a severe loss of reputation. To secure the entire network, an assessment has to be conducted at each layer and a continuous cyber security process followed.

Our solutions support the functional requirements highlighted in the IMO2021 regulation regarding cybersecurity. The IMO has indicated that maritime companies must be able to demonstrate that they follow the NIST cyber security framework of Identify, Protect, Detect, Respond and Recover.



Cyber risk management should: IDENTIFY key stakeholders' responsibilities, identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety. Establish technology such as a firewall and anti-virus and procedures to PROTECT against a cyber incident and ensure operational continuity. Combine more advanced network-based hardware and software solutions and expertise to DETECT vulnerabilities. All while implementing procedures to RESPOND to and RECOVER from cyber security incidents, using a contingency plan that is assessed and re-evaluated regularly, as well as by giving regular training.

Key Facts

- Vessels not compliant with the IMO 2021 Safety Management System (SMS) regulation risk detention by port control
- The most common motivation of cyber attacks is financial gain (29%), using ransomware, card theft and illicit transfers
- The second most frequent objective is data theft (espionage, intellectual property)
- Vessel operators have reported a 400% increase in cyber attacks since the coronavirus pandemic began
- On average, advanced attackers are on a network for almost three months before being detected
- Business disruption costs of a network outage caused by a cyber attack are likely to exceed $50k per vessel per day
- Most hull insurances exclude consequences of cyber attacks

Sources: Allianz Safety Shipping Review 2020, FireEye M-Trends 2020

Our comprehensive portfolio of cyber security solutions means whatever your business, we can provide the best-fit, most suited option for your requirements

- 24/7 Network protection and support
- IT Infrastructure and software management
- Uncover advanced cyber-attacks explicitly targeting your company
- Advanced, satellite-optimised end-point Protection
- Cyber Competence Expertise
- Smart, integrated, remote communications management

Maintain full control and ensure IT and OT security

Marlink's CyberGuard security solutions portfolio effectively protects your vessel from cyber risk



Your first layer of defence: Sealink Network Security

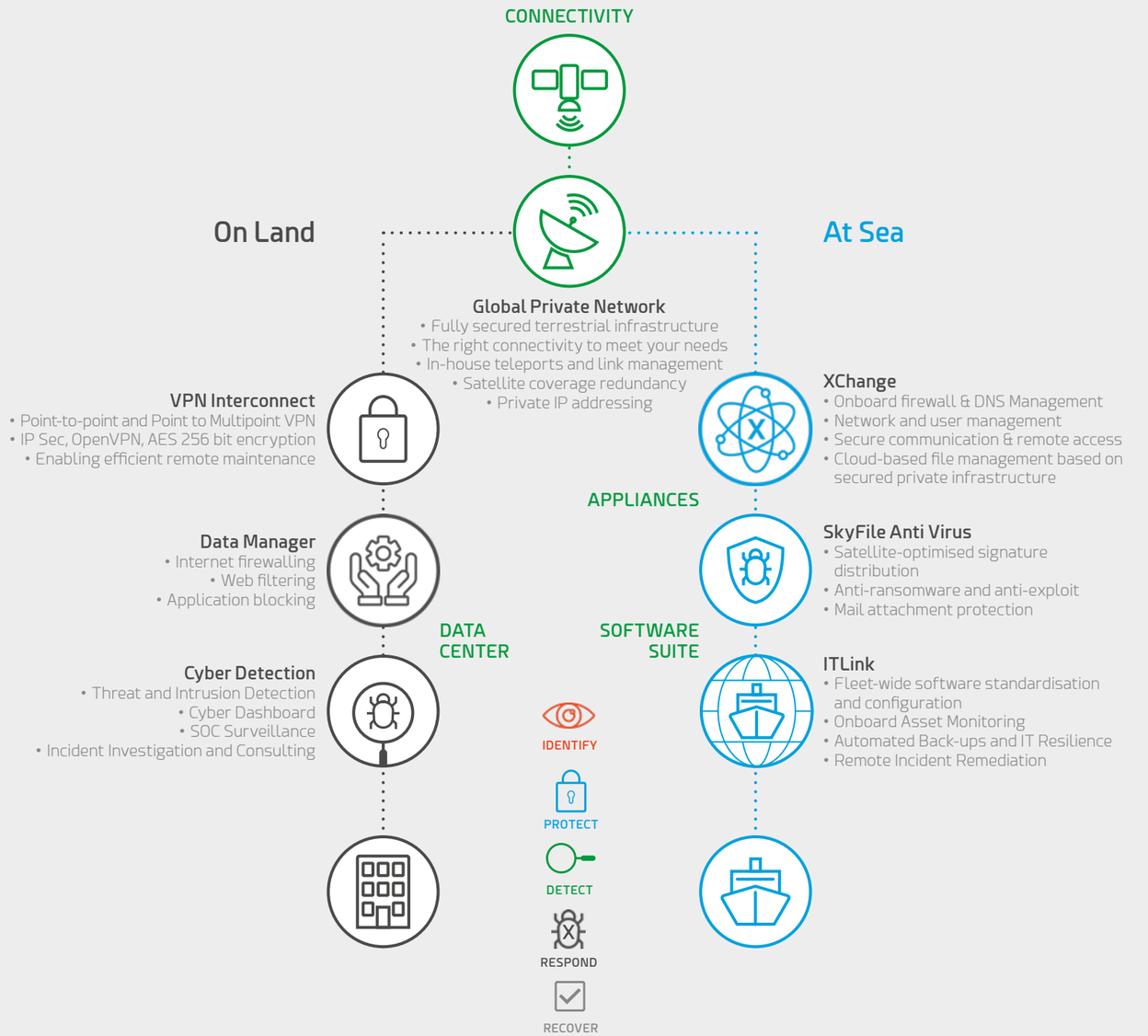
Your cyber security begins with the network layer, and Marlink makes continual, extensive efforts to ensure our core network is secure by design:

- Marlink secures your onboard traffic by providing private IP ranges to onboard networks.
- By standard, Marlink uses Port Address Translation (PAT) at the internet gateway, preventing traffic originated from the Internet from reaching the vessel.
- Marlink equipment is managed via out-of-band networks that are not connected to the Internet, meaning an attacker could not take control of Marlink network equipment. All equipment management access is authenticated and encrypted.
- Marlink has a dedicated security organisation that supervises security policies, logs and alarms.
- Marlink conducts periodic penetration testing provided by a third party security organisation.
- To avoid illegitimate bandwidth use, normal internet access via Marlink's VSAT network does not allow shore-to-ship traffic to be initiated. If a public IP is given, the customer is asked for a list of authorised IPs for access control.
- Each customer's corporate network traffic is kept private and segregated with tunnels and/or dedicated VRFs. This forms a private network dedicated to each customer.
- Marlink can apply generic or dedicated security rules in its firewalls. Firewalls keep up to date malware signatures and content lists from multiple sources.
- On top, our CyberGuard suite of cyber security solutions offer an additional layer of security, from scanning network traffic to automating anti virus updates.

Addressing Cyber Risk - Marlink's CyberGuard Solutions Portfolio

	SCOPE	CYBERGUARD SOLUTION	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
SECURITY LAYERS	Data Encryption	**VPN Interconnect** Secure end-to-end transmission		●			
	Fleet-wide	**Data Manager** Shore based gateway		●		●	
	Onboard Network	**XChange** Centralised communication platform	●	●		●	
	Onboard Computers	**SkyFile Anti Virus** Essential antivirus layer onboard		●	●	●	
	Fleet-wide	**Cyber Detection** Network threat monitoring service			●	●	
	Onboard IT	**ITLink** Comprehesive IT management	●	●		●	●

Your Cyber Security partner for end-to-end protection







Scope: Data Encryption

Scope: Fleet-wide

Scope: Onboard Network

VPN Interconnect

PROTECT

Marlink Virtual Private Network (VPN) solutions offer encrypted communication, protecting from sniffing attacks during data transmission over public internet. Marlink provides a variety of interconnect and secured on demand access solutions such as:

- On Demand VPN to establish a secure remote connection to equipment or computers on-board, typically used for debugging, maintenance and configuration
- Permanent VPN to secure regular transport data traffic to a corporate network

Key Benefits:

- **Flexible security protocols:** flexible integration with multiple options (IPsec, OpenVPN)
- **Remote maintenance:** essential and inexpensive tool for managing onboard networks (XChange Universal Remote Access)
- **Universal Connectivity:** supports Sealink VSAT, Fleet Xpress, FleetBroadband, Iridium OpenPort and Certus and other broadband connections like Marlink´s 4G services
- **Saves time and costs:** no need for additional hardware or intervention on board

Data Manager

PROTECT RESPOND

Data Manager provides a variety of versatile features to make managing data traffic more efficient, including web filtering, enhanced firewall and more.

Managed via a secure and simple online portal, the solution combines complex and powerful IP management capabilities with administrative simplicity for ease of use and secure communications.

Key Benefits:

- **Security:** full security package to protect your terminals from internet attacks
- **Flexibility:** customisable features like firewall, web filtering
- **Universal Connectivity:** supports Sealink VSAT, Fleet Xpress, FleetBroadband, Iridium OpenPort and Certus
- **Simplicity:** no installation required, all standard web browsers supported
- **Concealed Network:** hides your vessel from public Internet and potential cyber attackers

Example Scenarios

Threat	Solution
A third-party intercepts confidential data sent over the public internet	**Marlink provides several satellite optimised end-to-end as well as terrestrial VPN Solutions routing traffic over secure private network lines**
A crew member visits undesired / dangerous websites	**Data Manager offers a large number of categories simplifying access management to Websites**

XChange

IDENTIFY PROTECT RESPOND

Marlink's integrated communication management platform, XChange has been expertly designed to empower your connectivity and manage all satellite networks (VSAT and MSS). Among its many features, within the context of IT, OT and Network Security, XChange supports the following:

Segregated LAN Management - The network is split into multiple local networks (LANs) typically separating business from crew communication and avoiding infection caused by private equipment.

User Access Management - XChange acts as a gateway permitting or declining access to applications depending on preset policies and access rules - managing who is able to communicate, through which terminal, at what time and for how long.

Multi-Stage Firewall - XChange includes 2 firewall stages, which filter IP-based data communication based on ports, IP protocols and addresses:

- **Level 1: Terminal level Firewall -** block certain traffic types per terminal (VSAT, MSS)
- **Level 2: User-group Firewall -** determines traffic type per specific users or groups of users
- **Level 3: Combined with Data Manager -** provides a third layer of firewall protection at shore

XChange Cloud - Avoiding exposure to risks by the public internet, XChange Cloud is a Secure Content Delivery infrastructure from Shore to Vessel. This service streamlines and enhances business, logistical and vessel operations by providing a reliable, easy to manage platform to share and automatically synchronise important files of any size or type throughout a fleet.

Key Benefits:

- **Secure:** multi-stage firewalls guard what traffic is routed to and from the vessel
- **Access Control:** set group policies on access rules, time frames and time limits
- **Split networks:** separate and prioritise business critical communication over crew data traffic, thereby reducing cyber threats to operations
- **Full Remote Management:** administer XChange remotely or locally
- **DMZ Content Delivery:** transfer and synchronise files using XChange Cloud

Example Scenarios

Threat	Solution
A malware infection spreads from the crew welfare to the operational business network	**XChange splits the physical network into multiple LANs ensuring business remains unaffected**
A crew member connects an unauthorised device onboard, which may potentially be infected by viruses	**XChange can limit access to known pre-entered MAC addresses of approved devices only**
An onboard device is accessed remotely via a public, static IP exposing the device to cyber attackers	**Instead of using a public IP, URA uses secure authentication and an encrypted connection to remotely access devices**



Scope: Onboard Computers

SkyFile Anti Virus

PROTECT DETECT RESPOND

SkyFile® Anti Virus is Marlink's complete anti-virus software package, providing remote onboard PCs with protection against viruses and other external threats. Fully automatic anti-virus updates, notification and version verification ensure you keep your computers and LAN safe even while at sea.

Augmented specifically for satcom connectivity, SkyFile® Anti Virus combats a wide range of threats such as viruses, Trojan horses and other malicious software (malware).

As part of SkyFile® Anti-Virus Premium, ransomware and exploit mitigation enables even more advanced endpoint protection. Eliminate malware, prevent exploit vulnerabilities and get a deep clean on any potentially hidden malware using our premium options.

SkyFile® Anti Virus works seamlessly with one of Marlink's most popular solutions - SkyFile® Mail to deliver daily malware signature updates. With more than 40,000 mariners utilising the service daily, SkyFile® Mail provides reliable and cost-effective email, fax and SMS messaging. Viruses and spam are eliminated based on typical properties (blocked HELO, grey listing, etc.) reducing email threats - the most growing method of cyber intrusion.

Key Benefits:

- **Security:** Reliable detection using Sophos-based engine
- **Ransomware protection:** detects and blocks even brand new ransomware threats
- **Cost efficient:** several compressed low data volume anti-virus updates per day
- **Universal Connectivity:** Supports Sealink VSAT, Fleet Xpress, FleetBroadband, Iridium OpenPort and Certus

Example Scenarios

Threat	Solution
A crew member connects a malware-infected USB stick to the bridge PC	**SkyFile Anti Virus detects and blocks viruses and other malware such as Trojan horses or spyware using a Sophos-based virus detection engine**
New ransomware which is not yet detected by the anti-virus signatures is executed on a computer	**SkyFile Anti Virus Premium uses behavioural monitoring to detect and block even new, previously unknown ransomware**
Fraudulent spam and phishing emails are received onboard which direct crew members to websites stealing confidential information	**SkyFile Mail scans mail attachments for infections and moves spam to quarantine before delivery to the vessel**

Scope: Fleet-wide

Cyber Detection

DETECT RESPOND

Marlink's Cyber Detection service monitors your communications for any threats that may be putting the confidentiality and continuity of your business operations at risk.

Threat Monitoring: the service monitors all network traffic around the clock and provides an overview of threats affecting your vessels through an intuitive, web-based dashboard. Each threat description gives practical counter-measure suggestions to remedy the incident, while notifications on critical threats may be received by email.

The Marlink Security Operations Centre (SOC) is operated by highly-skilled cyber security experts. Being focused exclusively on maritime satellite communications enables our agents to understand and track how attackers operate and impact shipping companies.

Full visibility: Cyber Detection can uncover a multitude of threats and is continually evolved to keep up with the latest threat landscape, including:

- Malicious applications
- Abusive usage
- Intrusion attempts
- Confirmed intrusions
- Social engineering, etc.

Versatile Package Options: Choose your ideal service package in accordance with your preferences and in-house resources:

- **Entry Package -** full Cyber Dashboard access, with with suggested standard counter-measures following the detection of threats.
- **Business Package -** full Cyber Dashboard access with our Maritime SOC performing managed threat validation, contextual countermeasure suggestions as well as being your point of contact for any questions and investigations.

Key Benefits:

- **Threat detection:** uncovers advanced cyber-attacks targeting your company
- **Maritime SOC Monitoring:** dedicated maritime cyber surveillance expertise
- **Actionable reporting:** clear alert description and suggested counter-measures
- **IT and OT conformity:** detects abusive usage onboard circumventing safeguards
- **Scalable:** subscription model, no investment required

Example Scenarios

Threat	Solution
A targeted attack exploits a unique weakness and stays undetected for a long time	**Marlink's Security Operations Center (SOC) is specialised in hunting sophisticated 0-day attacks**
A crew member finds a method to access a blocked application or website bypassing all protection solutions	**In tune with your IT and OT Policies, the Cyber Dashboard reports any breach even if the onboard protection is inactive**
A device has been infected by malware and is wasting bandwidth, slowing down communication onboard	**Marlink's Cyber Detection Service reports on infected devices in the Cyber Dashboard**



Scope: Onboard IT

ITLink

IDENTIFY PROTECT RESPOND RECOVER

ITLink is a unique IT operational platform and solution to standardise, simplify and automate your vessel IT environment, permitting central remote management, IT resilience, fast migration, and effective operation of IT services across the fleet.

The solution combines expert advice and proactive support, with practical tools for system design, installation, logistics, and operational services. **ITLink can enable automatic installation, reinstallation and repair of applications, with a complete reinstall of a computer possible with no manual configuration, no data loss and no intervention onboard.** ITLink can be adopted in two ways, as best fits your operations and budget:

Advanced Solutions:

ITLink Pro - working in partnership with your own IT team

ITLink Managed - outsourced to Marlink to reduce dependencies on your own IT resources

ITLink Pro and Managed include:

Dashboard: presents fleet-wide health status for critical components on board.

Appstore: for easy management of business applications.

BackUp: enables proactive, vessel-optimised protection of business-critical data through automated synchronisation, and complete data recovery in case of an incident.

Disaster Recovery: enables full restoration of entire vessel server to either the same hardware, a dedicated spare server or a designated low computer without requiring a costly and complex dual server design.

Additionally, ITLink embeds incident prevention barriers, such as blocking USB storage devices, revoking local admin rights, access control management, and so on; reducing the probability of unwanted or critical situations, and reducing the consequences and damage caused by a cyber incident.

Entry Solutions:

ITLink Monitor - providing simple and secure fleet IT monitoring.

ITLink App Deployer - enables you to eliminate the hassle from application distribution.

Key Benefits:

- **Full configuration control:** centrally managed; track changes, upgrades and the operational status of vessels' IT
- **IT resilience & recovery:** proactive safeguarding of all vulnerable data and automated recovery if needed
- **IT Standardisation:** support in achieving harmonised computer and server configuration across the fleet
- **Reduce onboard workload:** routine tasks are automated and no specialised onboard IT competence is required
- **Proactive support:** from vessel IT experts with the capabilities to promptly resolve challenges

Example Scenarios

Threat	Solution
Outdated software contains security vulnerabilities which allow attackers to enter the network	**ITLink monitors software on all PCs onboard. Updates to mitigate known vulnerabilities can swiftly be distributed to the fleet**
A crew member has modified a PC's configuration for a leisure application without approval of the IT department	**ITLink will present installation activity via the monitoring tool to enable removal of unapproved applications**
A malware has modified the IT system and/or deleted important business documents	**ITLink supports automated Windows OS & applications repair, restoring full endpoint functionality via simple, user-friendly procedures. Backup saves all business-critical data to external device(s) according to agreed data retention policy**

Creating a secure culture

Today's shift towards increasing interconnectedness at sea is continuing to enable significant efficiency gains and new capabilities for maritime operations. Running in parallel to this trend is an increase in vulnerability to cyber-attacks within the maritime industry.

Although historically not considered part of the critical infrastructure sector, considering that now more than 90% of global trade is carried by sea, maritime has increasingly become a cyber target, as proven by recent high-profile, damaging cases.

To remain safe and competitive, ship operators should aim to employ not just a short-term incident resolution, but a blend of tools and complementary solutions to cover all aspects of the Protect, Detect and Resolve process.

Marlink's more than 70 years' experience in the maritime sector has been harnessed into designing sophisticated, but straightforward and easy to roll-out solutions to precisely fit this purpose.

The Human Element

In addition to technical cyber security solutions, it is essential to create awareness among staff through regular training and a clearly defined IT system usage policy. Whilst the technology and solutions onboard are essential elements to addressing cyber security, only by combining training, technology, regular reviews of business processes and implementation of the correct policies can a shipping company hope to reduce its cyber risk level.

Protecting Your Business in the Digital Age

- Comprehensive solutions portfolio
- Focus on ongoing protection, detection and threat resolution
- Efficient, quick deployment technology
- Remote management from shore
- Optimisation for satellite environments
- Customer consultants located in regional offices worldwide
- Support available 24/7/365
- Regional, cultural and technical understanding

Are you IMO2021 Compliant?

Applicable to commercial ships with over 500 gross tonnage, the IMO resolution (MSC 428, 98) confirmed all shipping companies need to have cyber security in their safety management system. Flag states are encouraged to check this in the first annual audit after January 2021.

Our solutions support all the functional elements of the IMO2021 regulation regarding cyber security.

Contact us for a free consultation.

Marlink is a true partner, who goes Above and Beyond to help you run your remote operations in ever smarter, more profitable and sustainable ways to give you the competitive edge.



Marlink Service Desk

EMEA: +33 (0)1 70 48 98 98
Americas: +1 (310) 616 5594 | +1 855 769 39 59 (toll free)
Asia Pacific: +65 64 29 83 11

Email: servicedesk@marlink.com
Web: www.marlink.com

MARLINK
ABOVE AND BEYOND

CG 02 21