inmarsat

The mobile satellite company

Fleet Secure – Key benefits

1 Identifies risk and threats by detecting devices on the local network that do not have Fleet Secure Endpoint installed

2 Blocks and prevents cyber attacks based on file detections, intelligent behavior analysis and low-level system calls on the network

3 A full report can be created on a vessel containing a record of all devices connected to the network, their hardware and software that is installed

4 24/7 Monitoring by engineers in a Security Operating Center

5 Alerts can be created to E-mail you when events happen onboard, such as virus detections or outdated software

Pacific Gas Case Study

Pacific Gas (Hong Kong) Holdings Limited provides integrated supply chain services for a full range of clean energy and its derivative by-products in the international market.

Pacific Gas has ensured that upgrading to Fleet Xpress is supported by Fleet Secure Endpoint to provide protection against cyber attacks and meet IMO 2021 cyber risk regulations.

The largest Liquid Ethylene Gas (LEG) ship owner in China has installed Fleet Xpress connectivity from Inmarsat, the world leader in global, mobile satellite communications on all its vessels. This will also include Inmarsat's Fleet Secure Endpoint, the new line of defence in the multi-layered strategy to protect owners against cyber threats.

A fast-track transformation by Pacific Gas from specialised regional player to global trading partner has been matched by new connectivity commitments that support and protect its ambitious growth.

Initially acquiring second-hand tonnage from its launch in 2013, subsidiary Pacific Gas quickly moved into newbuilding, taking delivery of eight VLGCs in 2016-2017, while the last of five new Liquid Ethylene Gas (LEG) carriers will join the fleet shortly. Pacific Gas will offer capacity to carry 3 million tons of cargo annually, but it has already announced plans to expand into the LNG carrier and VLEC segments and add Houston to existing offices in Shanghai, Singapore and Mumbai.

The plans have been anticipated by a fleetwide connectivity upgrade that supports a more global outlook, with Pacific Gas choosing the bandwidth, coverage, guaranteed performance and 24/7 support available via Inmarsat Fleet Xpress. The commitment covers all operational ships and future vessel takeovers.

"With our growing dependence on technology and providing open internet access we could be susceptible to cyberattacks, so we need more than a conventional anti-virus to protect our systems 24/7 and from the various kinds of evolving threats"

Captain Tao Yong, Vice President Fleet, Pacific Gas

New levels of connectivity and performance with Fleet Xpress

"The reliability of Fleet Xpress has allowed us to scale our digital activities and complement our new ship management software that we installed to help resource planning on vessels," says Captain Tao Yong, Vice President Fleet, Pacific Gas. "Internet access at sea is also vital for crew welfare and essential to attracting and retaining talented crew."

Fleet Xpress replaces "a local service that had regional coverage and a metered plan," he says. "Given our business growth in international markets our bandwidth needs changed; our need for seamless global mobility and reliability is being met through Inmarsat's dual satellite constellation and unlimited back-up, guaranteed performance with high uptime, and round the clock management, monitoring and global support."

Stable connections are vital for a company continuously monitoring its ships remotely using CCTV for security, for example.

"With real-time data exchange, vessels become an extension to our shore office and we base our operational efficiency and performance gains on continuous monitoring and real-time upgrades and assistance," adds Capt. Tao Yong. Fleet Xpress is bringing "quicker turnaround in operational decisions as shore office and vessels are always connected".

Ensuring cyber resilience at sea

Like other forward-looking ship owners, Pacific Gas is fully aware that always-on connectivity and greater commitment to digitalisation also creates new requirements when it comes to protecting ships against the cybercriminals.

"With our growing dependence on technology and providing open internet access we could be susceptible to cyberattacks, so we need more than a conventional anti-virus to protect our

systems 24/7 and from the various kinds of evolving threats," says Capt. Tao Yong.

Pacific Gas included Fleet Secure Endpoint in its plans - Inmarsat's new line of defence against cybercrime.

> Fleet Secure Endpoint, winner of the Safety at Sea Award 2019 for Best Security Product of the Year, powered by ESET Endpoint Security and Port-IT, protects desktop computers and other systems connected to a vessel's network.

Fleet Secure Endpoint monitors ship systems for security breaches introduced at 'endpoints', either by malicious software or by a new crew device with no security installed, reporting a 'rogue node' and isolating it from the rest of the network until issue resolution. Powered by ESET Endpoint Security – recognised for its high performance by industry authority Gartner Inc. - Fleet Secure's advanced monitoring is distinguished for offering the user a greater sense of control and awareness over their environment.

"As a modern ship owner we ensure that all our vessels are equipped with state-of-the-art technology and security systems that complement Inmarsat's global, secure and reliable connectivity," says Capt. Tao Yong.

Where generic anti-virus software protects against spyware and phishing, Fleet Secure Endpoint includes a two-way firewall, web control, botnet protection, ransomware prevention, multi-engine scanning, network monitoring and asset inventory functions. It even includes its own health status alerting. Fleet Secure Endpoint can be applied to FleetBroadband and Fleet One, as well as Fleet Xpress.

In Pacific Gas, Peter Broadhurst, SVP of Safety and Security, Inmarsat, recognises "one of the growing number of quality operators adopting practical and pragmatic mitigation strategies that prioritise cybersecurity on shore and at sea. These companies see that the risks of a cyberattack on a vessel extend beyond loss of reputation; they include the risk of delays to the ship and cargo delivery, increased insurance premiums and blackmail."

Supporting compliance and upcoming regulation

Fleet Secure Endpoint will also support ship owners in their efforts to comply with International Safety Management (ISM) code revisions due in force from 1 January 2021.

Broadhurst points out:
"In practice, ISM code revisions will mean that, to comply, ships must be able to demonstrate what assets, personnel and procedures are in place onboard and ashore to deal with cyber risk issues, what happens if systems are compromised and who has control. Compliance will depend on having the right risk management, infrastructure and procedures in place. Fleet Secure Endpoint offers owners a scanning and record-keeping tool to document the efforts made to follow guidelines developed by industry organisations such as BIMCO, the International Chamber of Shipping and Intermanager."

> ## How to buy
>
> For further information, contact your Inmarsat Maritime Account Manager or email us at Maritime.security@inmarsat.com

inmarsat.com/gxfx