FORESCOUT

Solution Brief

Operational Technology

Securing Ship Automation & Control Systems

Using OT network monitoring to identify and mitigate cyberthreats and operational issues for the maritime industry

Shipping and maritime industries are increasingly dependent on integrated digital systems for everything from navigation to engine monitoring. Modern ships are floating cities and possess utility functions similar to them. They include everything from electric power generation to fuel dissemination to water treatment facilities. Other interconnected systems like HVAC, video surveillance, and automated safety controls are also present within a ship's network.

> By 2021, ship owners and managers must ensure that cyber risks are appropriately addressed in existing safety management systems. [1]

The Challenge

This shift toward automation and digital controls has improved efficiency, but these new technologies have also opened up ship networks to increased cyber and operational threats. Because of this, ship owners and managers risk having ships detained if they don't incorporate cyber risk management into ship safety by 2021, according to guidance issued by the International Maritime Organization (IMO). [1]

As one of the most safety-conscious industries, the maritime industry must follow strict classification rules and operational regulations to ensure that everything possible is done to prevent hazardous situations. Considering that the average maritime operation includes a medley of advanced sensors, systems and applications, the monitoring and security management of these applications is a monumental task.

Maritime operators need to be able to quickly collect and aggregate security and operational data from all their ship control and automation systems to maintain safety and operational reliability, and keep up with an evolving threat landscape.

The Maritime Cyber Resilience Platform: SilentDefense

Forescout SilentDefense provides maritime operations with complete device visibility and advanced threat detection of all marine control networks and monitoring applications to enhance rapid remediation capabilities - from critical alarms to I/O and IP device networks. With SilentDefense, operators in port or out at sea can detect operational anomalies and threats before they lead to potentially dangerous incidents and help prevent them in the future.

The optional **Enterprise Command Center** (ECC) provides global visibility and risk management for a whole fleet of ships from a single pane of glass. The ECC transmits relevant data from the field up to the enterprise level to analyze any incident in detail, including the devices involved and context of the alert.

The benefits of SilentDefense extend far beyond conventional cybersecurity to offer asset owners in the maritime industry the power of complete OT visibility and system integration with legacy and new bridge control systems.

Solving Onboard Industrial Challenges

Ship Control Network Security:

- Protect navigation and GPS operations
- Identify and remediate ICS malware attacks
- Monitor unauthorized internet connections
- Enforce network activity and policy
- Uncover firewall and network misconfigurations

Network Access Control:

- Identify unauthorized or undesired user credentials
- Identify network intrusion attempts
- Implement policy enforcement with existing infrastructure like firewalls
- Detect weak links (e.g., connection to the Internet)

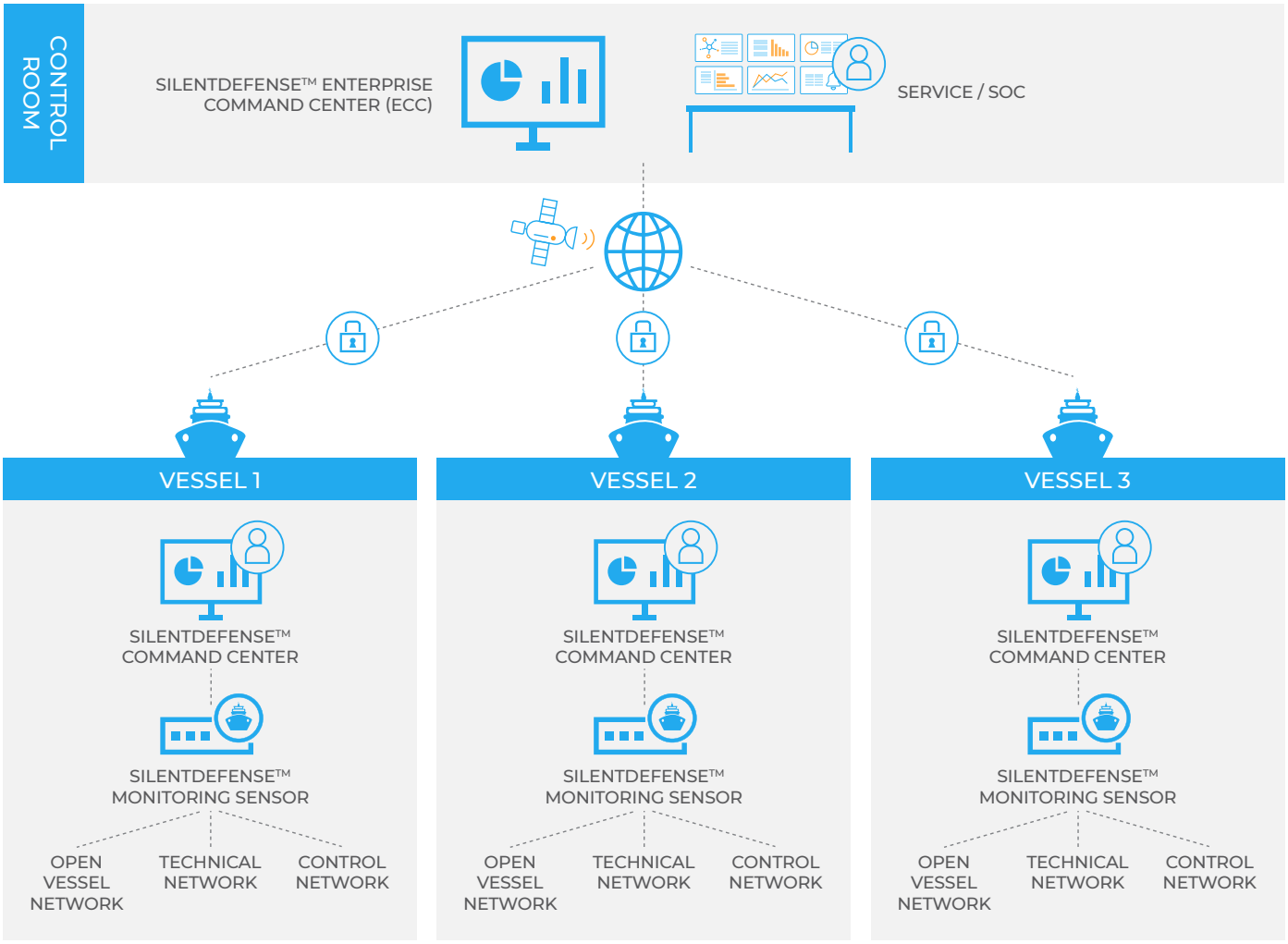
Peripheral Systems (CCTV / HVAC):

- Detect unpermitted system activity / user tampering
- Identify communication flow and device anomalies
- Assess risk level of communication flow and anomalies
- Customize alerts and remediation paths using variable analysis

Ship Control Network Operations:

- Identify new and changed device settings
- Detect known and unknown cyber threats with multifactor threat detection
- Automate response to indicators of compromise (IoCs) with:
  - Policy enforcement with firewall
  - Alert management and remediation path
  - Network user access control and monitoring


Enterprise Deployment for Cruising or Shipping



Each ship is an independent and autonomous system reporting to the ECC.

Complete Visibility Into Ship Systems

SilentDefense can identify and help remediate a full range of both cyber and operational threats to ships, including, but not limited to:

- Passive detection and classification of hosts
- Cyberattacks (DDoS, MITM & Scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior / policy changes
- Device malfunction misconfiguration
- New and non-responsive assets
- Corrupted messages
- Unauthorized firmware downloads
- Insecure protocols
- Default credentials and insecure authentications
- Logic changes

SilentDefense Use Cases for the Maritime Industry

Asset Visibility and Monitoring

SilentDefense provides continuous asset visibility across OT networks and sites. It automatically builds a detailed network map with rich asset details and automatic grouping by network and/or role, provided in multiple formats such as Purdue level and communication relationship. SilentDefense uses a wide range of discovery capabilities that include:

- Patented deep packet inspection of 130+ IT and OT protocols
- Continuous, configurable policy and behavior monitoring
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems

Asset Configuration Management

SilentDefense automatically collects a wide range of OT asset information, logging all configuration changes for security analysis and operational forensics. Discoverable details include:

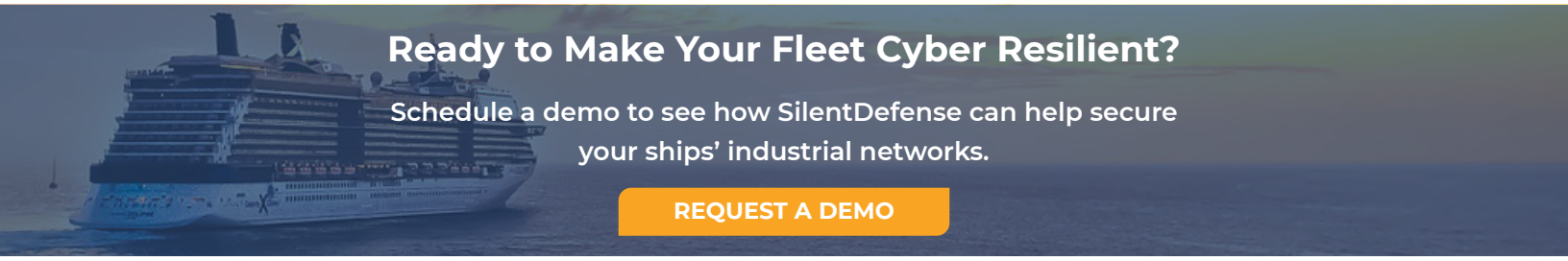
- Network address
- Host name
- Vendor and model of the asset
- Serial number
- OS version
- Firmware version
- Hardware version
- Device modules' information

Risk Management and Compliance

Proactively identify vulnerable OT assets to prioritize mitigation strategies with the Asset Risk Framework, the first centrally available 'impact-based' risk tool for ICS/OT networks. It saves time, improves SOC and analyst effectiveness and reduces risk by automating security and operational risk analysis. SilentDefense also includes powerful dashboards, analytics, and out-of-the-box reporting tools that simplify compliance with key standards, including ISA 99/IEC 62443 and the NIST Cybersecurity Framework.

Threat Detection & Incident Response

Automate threat detection, containment and remediation with alert investigation and response tools. Dashboards and widgets enhance user collaboration, while rich alert detail supports root cause analysis and expedites effective, efficient response. The Enterprise Command Center (ECC) allows users to zoom in on alerts from any ship in their geo-distributed fleet to analyze an incident in detail, including devices involved and context of the alert.



[1] IMO (International Maritime Organization); http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com