Digitization

Digitization focuses on connecting "things," such as objects and machines, to a computer network, such as the Internet

DX

is the integration of digital technology IT into all areas of a business, resulting in fundamental changes to how businesses operate and how they deliver value to customers.
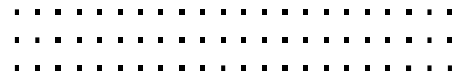
[Digital Transformation]

SX

is the integration of security into all areas of digital technology, resulting in a Security Architecture that provides a Continuous Trust Assessment.

[Security Transformation]

Critical Infrastructure

Critical infrastructure (or critical national infrastructure (CNI) in the UK) is a term used by governments to describe assets, Systems, Networks that are essential for the functioning of a society and economy.

A Critical Infrastructure (CI) consists a set of systems and assets, whether physical or virtual, so essential to the nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination of these

What is OT / IOT?

Field Sensors/Actuators are diverse physical devices that are deployed on or near physical devices and processes. Sensors **measure** physical attributes like temperature, voltage, rpm. Actuators turn equipment such as motors, pumps, breakers on and off. They are sometimes referred to informally as the 'Industrial Internet of Things (IIoT)'.

Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the industrial environment.

Supervisory Control and Data Acquisition (SCADA) refers to a system that collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data.

Industrial Control Systems (ICS) play a main role in OT and includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs).

Terminology - Introduction

- Critical Infrastructure (CI)
- Operational Technology (OT)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Field Sensors/Actuators

CI | OT | ICS | SCADA | Field Sensors/Actuators
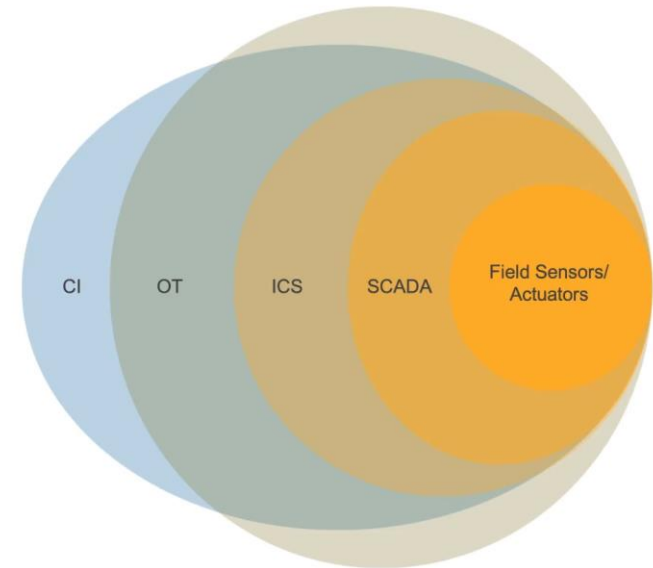
IoT - Digitization

- Internet of Things (IoT), also known as **Internet of Everything** (IoE) refers to the network of devices with an IP address that have the capability of sensing, collecting and sending data using embedded sensors, communication hardware and processors

- In IoT, a **thing** is referred to as the device that is **implanted on natural** or **man-made** or **machine-made** objects and having the functionality of **communicating over the network**
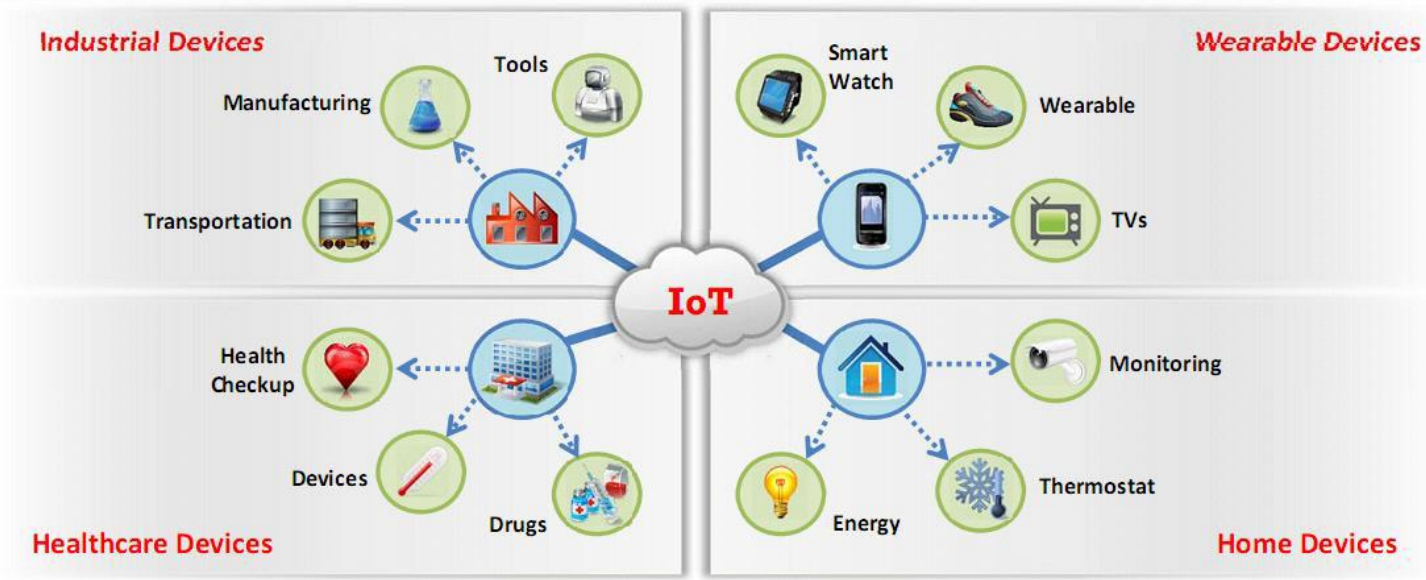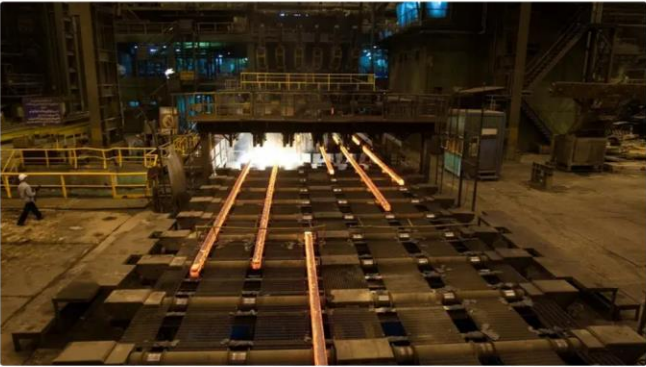
Attack Scenario
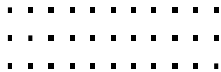
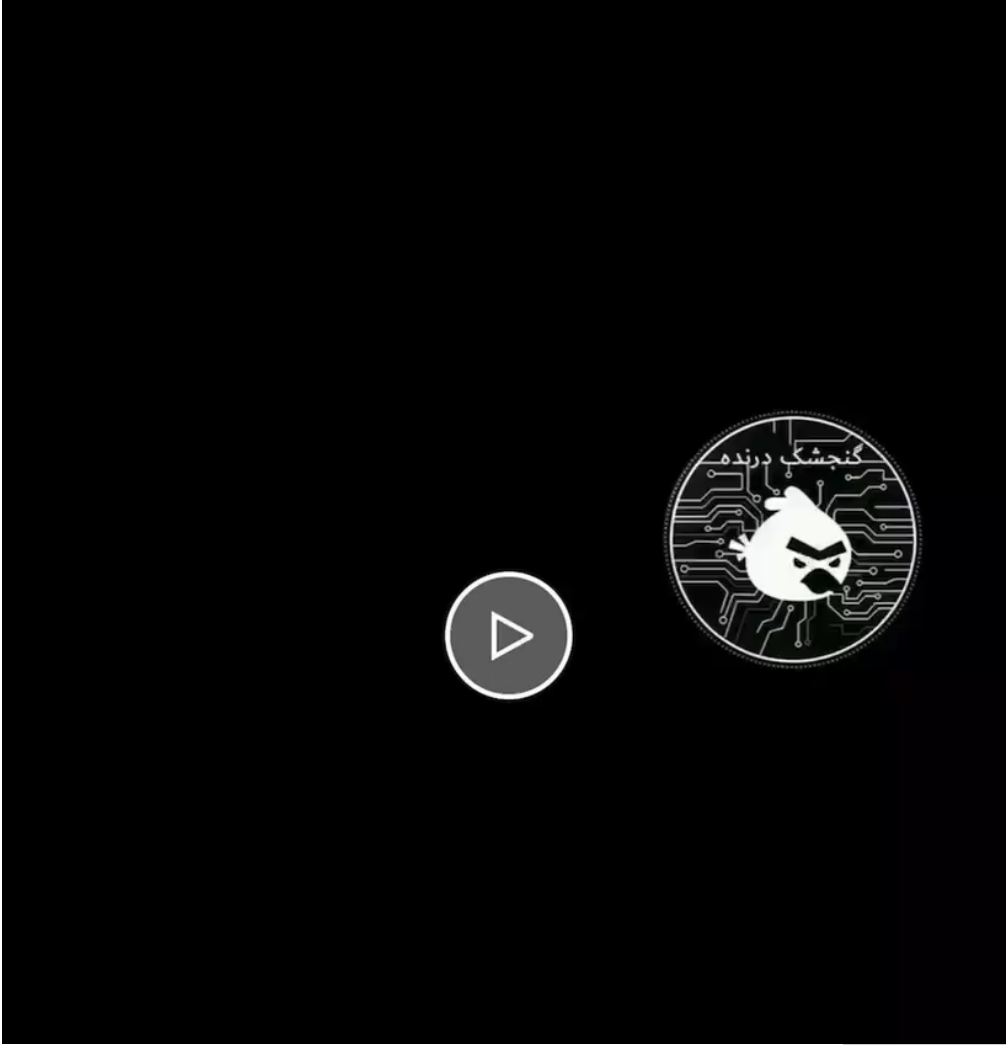Cyberattack forces major Iran steel company in Khuzestan to halt production

A view of the steel facility in Ahvaz, Khuzestan province, 882 km (548 miles) southwest of Tehran. (File photo: Reuters)

The Associated Press

Published: 27 June ,2022: 01:16 PM GST
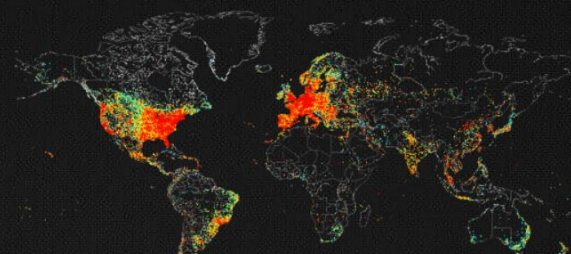Updated: 27 June ,2022: 01:29 PM GST

SHODAN

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

📊 View Report   ⬇ Download Results   📊 Historical Trend   🗺 View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out **Gravwell**

customer networks and M&C devices

```
SNMP:
    Uptime: 459535149
    Description: SAILOR 900 VSAT
    Service: 72
    Versions:
        3
    Name: acu1
    Ordescr: View-based Access Control Model for SNMP.
    Contact: root@localhost
    Oruptime: 3
    Engine Boots: 1
    Engineid Data: 80001f88804d81e610ed88b663
    Enterprise: 8072
    Objectid: 1.3.6.1.4...
```

What Is a Smart Port?

A Smart Port is digital. "Smart" means "connected" being more attractive and innovative with more intelligence in a competitive sense.

Ports link vessels and goods with importers and exporters. They are a major node in global supply chain operations of the maritime industry and trade. Ports have now become entire communities and ecosystems.

Smart Ports encompass Big Data, Artificial Intelligence (AI), Internet of Things (IoT), blockchain technology, and 5G / Wireless technologies.

Why Do Smart Ports Matter?

1- The population is growing, ports are crowding, and with a globalized economy, goods need to move faster.

2- Everything is connected, smart, and to remain competitive in the shipping market and at capacity, you need your port to be green and smart.

3- Ports are also responsible for the safety and security of employees and affected stakeholders.

4- Collision prevention, protected environmental areas, environmental pollution prevention, and worker safety.

5- Increasing shipping traffic.

Everything is connected, so

Supply chain efficiency starts with securing port operations

Why is the Maritime Industry being Attacked?

The digital transformation initiative propelling Maritime 4.0 forward is revolutionizing the shipping industry. This digital revolution can make all the difference in ensuring a shipping company's future viability and competitive edge by way of optimizing ship operations and voyages, improving ship system efficiency, lowering its environmental footprint and reducing fuel consumption and costs. However, what does digital transformation actually entail for the shipping industry?

The Maritime Industry is a Cornerstone of National and Economic Security

"80 percent of global trade by volume and more than 70 percent of its value is being carried on board ships and handled by seaports worldwide, which represents a staggering role in the global economy."

The United Nations Conference on Trade and Development (UNCTAD)

Why is the Maritime Industry being Attacked?

- Increased networking and connectivity (e.g. ship-to shore communications, IT-OT connectivity, remote control of offshore and onboard operations, cloud applications, etc.)

- Ship bridges as automation control centers (e.g. navigation, cargo information or declaration, administrative data, etc.)

- Smart ships and intelligent fleets (e.g. route planning, unmanned shipping, the EU Sea Traffic Management initiative seeking to synchronize shipping operations using communications, networking and Big Data)

- Intelligent and linked sub-systems using industrial automation (e.g. ballast water system, alarm and monitoring systems, etc.)

- Unifying network technology for advanced ship systems(e.g. in the case of reefers, allocating ship costs according to the source rather than uniformly distributed)

The Maritime Industry is a Cornerstone of National and Economic Security

"80 percent of global trade by volume and more than 70 percent of its value is being carried on board ships and handled by seaports worldwide, which represents a staggering role in the global economy."

The United Nations Conference on Trade and Development (UNCTAD)

Who is targeting the Maritime Industry?*

Threat Actors

Foreign Sovereign States

Non State Entities

- Criminals
- Terrorists
- Pirates
- Organized Crime
- Activists
- Hacktivists
- Cybercriminals
- Spies
- Competitors
- Illegal Fishers

Insiders

- Employees
- Contractors
- Partners

*Source: "Trojan horse risks in the maritime transportation systems sector"— Journal of Transportation Security, May 2018

Which Systems are Vulnerable?

Targets

Shipboard Systems

- Ship Operations
- Access Control & Security Systems
- Communication Systems
- Crew Internet Access

Critical Control Systems

- Cargo Control Room & Its Equipment
- Level Indication
- Valve Remote Control
- Water Ingress Alarm
- Ballast Water
- Gas Liquefaction
- Fire Suppression System
- Engine Governor
- Power Management
- Alarm System
- Emergency Response System

GPS & Navigation Systems

- Bridge Systems
  - TGPS
  - ECDIS
  - DP
  - AIS
  - GMDSS
  - Radar
  - VDRs

What are the Consequences of a Cyber Attack?

Impacts on

- Shipment Efficiency (i.e. speed, cost, volume)
- Shipment Reliability (timely delivery with minimal loss)
- Cargo Legitimacy
- Fault Tolerance (withstand disruptions & failures)
- Data Legitimacy
- Environmental and Human Safety

Effects

- Loss of Business
- Fines and Penalties
- Reputational Damage
- Supply-Chain Disruption
- Global Economic Loss
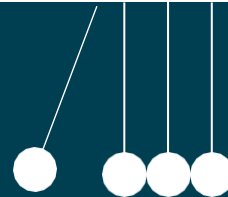- Compromised Health, Safety and Security

Examples

- Corrupting the records for a container's dimensions & weight resulting in an "uneven keel" which can sink the ship

- Compromising the fire suppression system and releasing CO2 which can kill crew

- Ransomware shutting down a bulk carriers's control board rendering the vessel inoperable

1
6

What is Driving The Maritime Industry to Adopt Stricter Cybersecurity Measures?

▪ The adoption of new technologies radically transforming the way the maritime sector does business at the cost of an expanding attack surface.

- Increased connectivity and reliance on digital components

- Increased levels of autonomous controls

- Globally accessible navigation systems

The need to address resolutions and regulations regarding cyber risks while protecting critical assets, infrastructure and data.

As OT and IT environments converge and become more connected and with cyberattacks increasing on the IT side, the vulnerability of the OT environment being exposed to these IT security threats is increasing.

IMO Resolution

Ship owners and managers risk having ships detained if they don't incorporate cyber risk management into ship safety

IMO INTERNATIONAL MARITIME ORGANIZATION

Getting to Know Your Environment

OT Environment

- Do you have remote monitoring for the following systems…

Cargo Control Room & Its Equipment	**Level Indication**	**Valve Remote Control**	**Water Ingress Alarm**	**Ballast Water**	**Gas Liquefaction**
Fire Suppression System	**Engine Governor**	**Power Management**	**Alarm System**	**Emergency Response System**	

- Are these systems accessible from shore based locations?

- Do these systems have SLAs that require remote monitoring?

Maritime 4.0 Requires a Security Transformation

It's clear from the continued breaches that the traditional methods of securing a shipping company's network no longer work. Traditional engineering methods have focused entirely on safety with little thought to security. As a result, both safety and security must be integrated in the engineering lifecycle to ensure ship safety from accidents and security from cyber threats.

In order to deliver a secure environment, shipping companies need to rethink their security posture and move towards a seamless and comprehensive cybersecurity strategy. As shipping companies adapt their IT and OT infrastructure to account for digital transformation, they must also undergo a security transformation to protect against the evolving cyber threat – the biggest risk to digital transformation. Fortinet provides companies in the maritime industry with a proactive and transformative approach to cybersecurity, the Fortinet Security Fabric which promises security that is:

Broad	Integrated	Automated
Visibility and protection of the entire digital attack surface to better manage risk	Solution that reduces management complexity and shares threat intelligence	Self-healing networks with AI-driven security for fast and efficient operations

The Fortinet Security Fabric Protects Maritime 4.0

Fortinet is well positioned to accompany shipping companies on their digital transformation journey with security transformation provided by the Fortinet Security Fabric. The Fortinet Security Fabric architecture (Figure 1) consists of a wide set of technologies that work together and are supported by a single source of threat intelligence to eliminate security gaps in the network and respond to any attack vector.

Key Benefits

- Secures the core infrastructure
- Ensures business activities are uninterrupted and sustained via internal segmentation
- Security interwoven throughout the different areas of a shipping company's network (i.e. both IT and OT and including third parties)
- Reduces network complexity and simplifies security
- Supports regulatory compliance
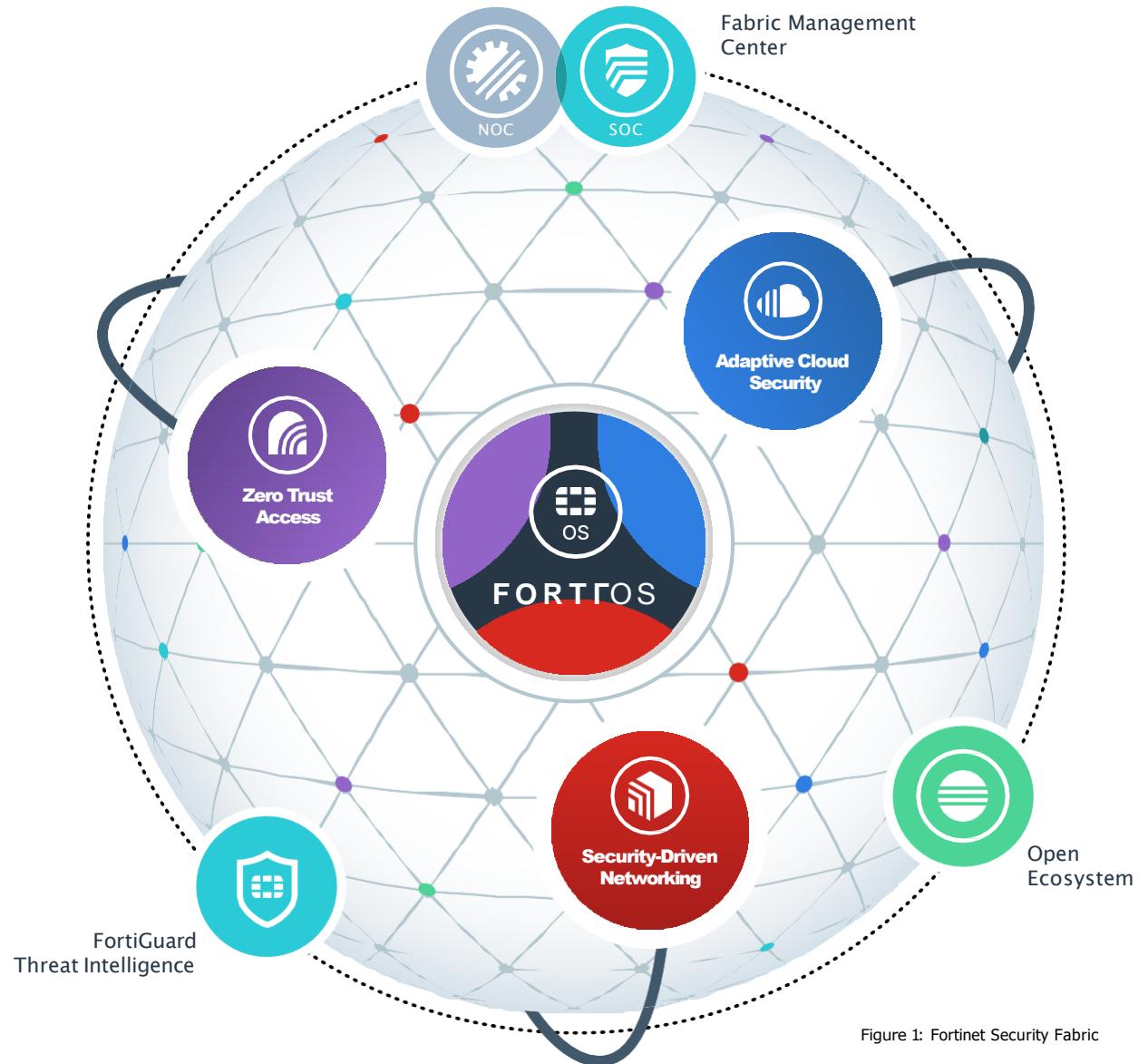- Provides visibility and detection across networks.

Figure 1: Fortinet Security Fabric

Step 1: Focus on Securing the IT Systems First (Vessel & Shipping Network)

Security-Driven Networking

Zero Trust Access

Adaptive Cloud Security

Fabric Management Center - NOC

Fabric Management Center - SOC

FortiGuard Security Services

Open Ecosystem

Shipboard Systems

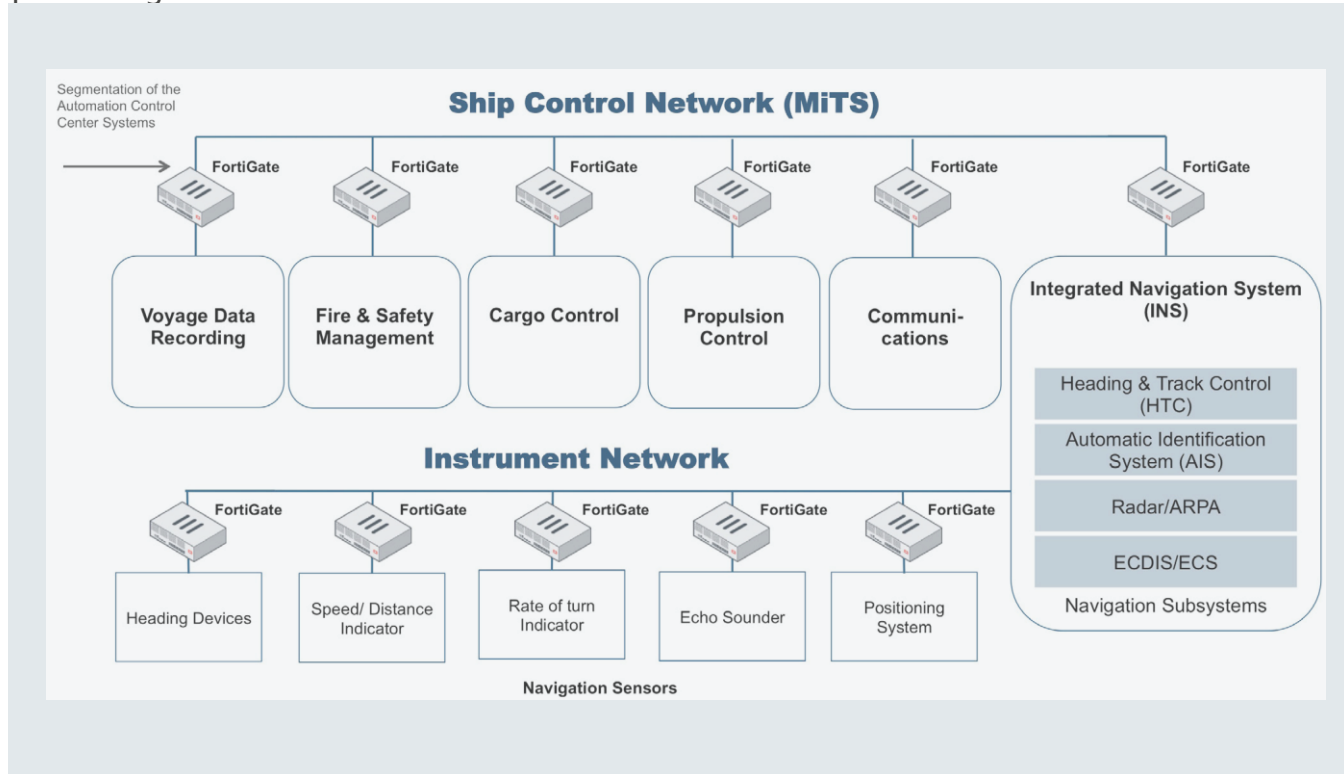IT

GPS & Navigation Systems

Key Benefits

- Secure the first point of attack
- Protect against advanced threats
- Control access and gain visibility

Secure the Vessel IT Infrastructure and Onboard Systems

Shipping networks are subject to a large number of cyber attacks. Once inside the network, hackers can easily move among resources while hiding from perimeter focused security which is why using firewalls
to segment the network is a critical component to network security. Layering a vessel's defenses allows prioritizing assets that need the

highest degree of protection without impacting performance. This dramatically improves visibility into possible attacks and provides complete internal segregation of data, resources and systems so that if one area of the network is compromised, other areas remain unaffected.

Segmentation of the Automation Control Center Systems

Ship Control Network (MiTS)

FortiGate — FortiGate — FortiGate — FortiGate — FortiGate — FortiGate

- Voyage Data Recording
- Fire & Safety Management
- Cargo Control
- Propulsion Control
- Communi-cations
- Integrated Navigation System (INS)
  - Heading & Track Control (HTC)
  - Automatic Identification System (AIS)
  - Radar/ARPA
  - ECDIS/ECS
  - Navigation Subsystems

Instrument Network

FortiGate — FortiGate — FortiGate — FortiGate — FortiGate

- Heading Devices
- Speed/ Distance Indicator
- Rate of turn Indicator
- Echo Sounder
- Positioning System

Navigation Sensors

Layer A Vessel's Defenses

- Increase Visibility
- Preserve Data Integrity
- Stop Threats from Propagating
- Ensure Marine Operations Continue Unaffected

Secure the Shipping Network & Eliminate Complexity

Fortinet's Network Security solution eliminates the complexity associated with securing the distributed nature of a shipping company's network environment. How? With the FortiGate Firewall, shipping companies can deploy cybersecurity across all parts of their shipping network while maintaining the same level of protection throughout. Depending on the location in the network and the required functionality, the solution provides shipping companies a range of deployment modes to meet their individual requirements.

Finally, for more comprehensive protection, the FortiGate seamlessly integrates with additional Fortinet solutions extending its overall capability to protect against advanced threats as well as secure the entire attack surface including satellite communications, wireless access, web applications, email systems, cloud environments and endpoints (e.g. mobile devices).
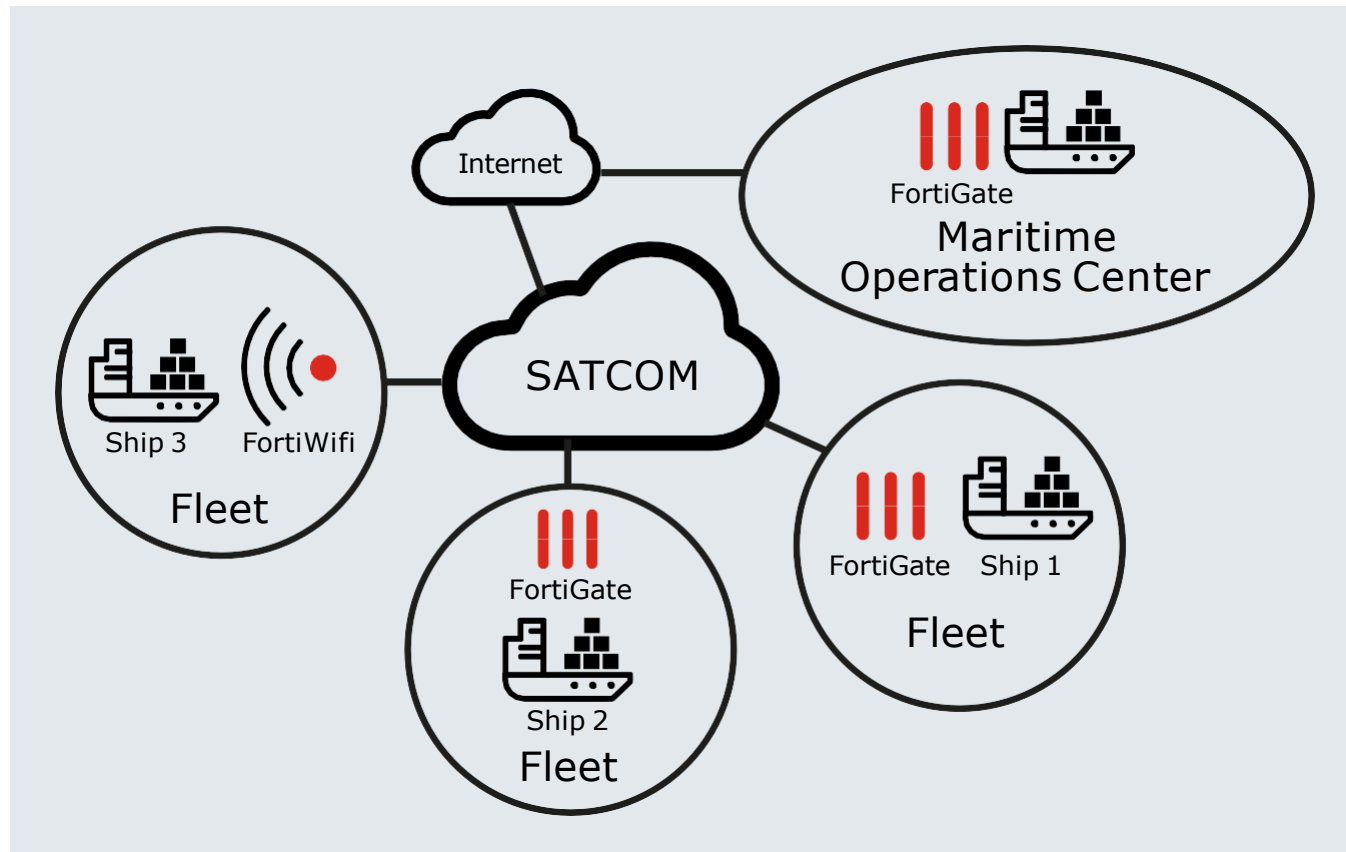

Network Security In Action

- High Performance & Scalable Network Solution
- Fine Tune Security Services (e.g. antivirus, application control, antispyware, antimalware, etc.)
- Multi-factor Authentication
- Access Control (e.g. device policies)
- Network Segmentation to Preserve Data Integrity
- Robust Visibility & Protection
- Service Availability

A Focus on Fortinet's Secure SD-WAN Solution

Today's shipping company typically spends a lot of time and resources on overly complicated security deployments that may not even be effective. As bandwidth requirements continue to increase at an alarming rate, many shipping companies are moving to the Internet to increase bandwidth and reduce costs which can raise serious security concerns.

Fortinet makes it easy to deploy and manage the right security in all the right places with our secure Software-defined WAN (SD-WAN) solution.

The solution links network and security paths across the world through the Internet, 3G/4G, or SATCOM links, making it a truly borderless infrastructure for a shipping company. It provides application visibility for encrypted traffic and smart load balancing which helps to reduce WAN cost without impacting the SLA for business applications. With Fortinet's SD-WAN solution, shipping companies can securely adopt digital business models and easily manage the growing volume of data and increasing number of endpoint and IoT devices.
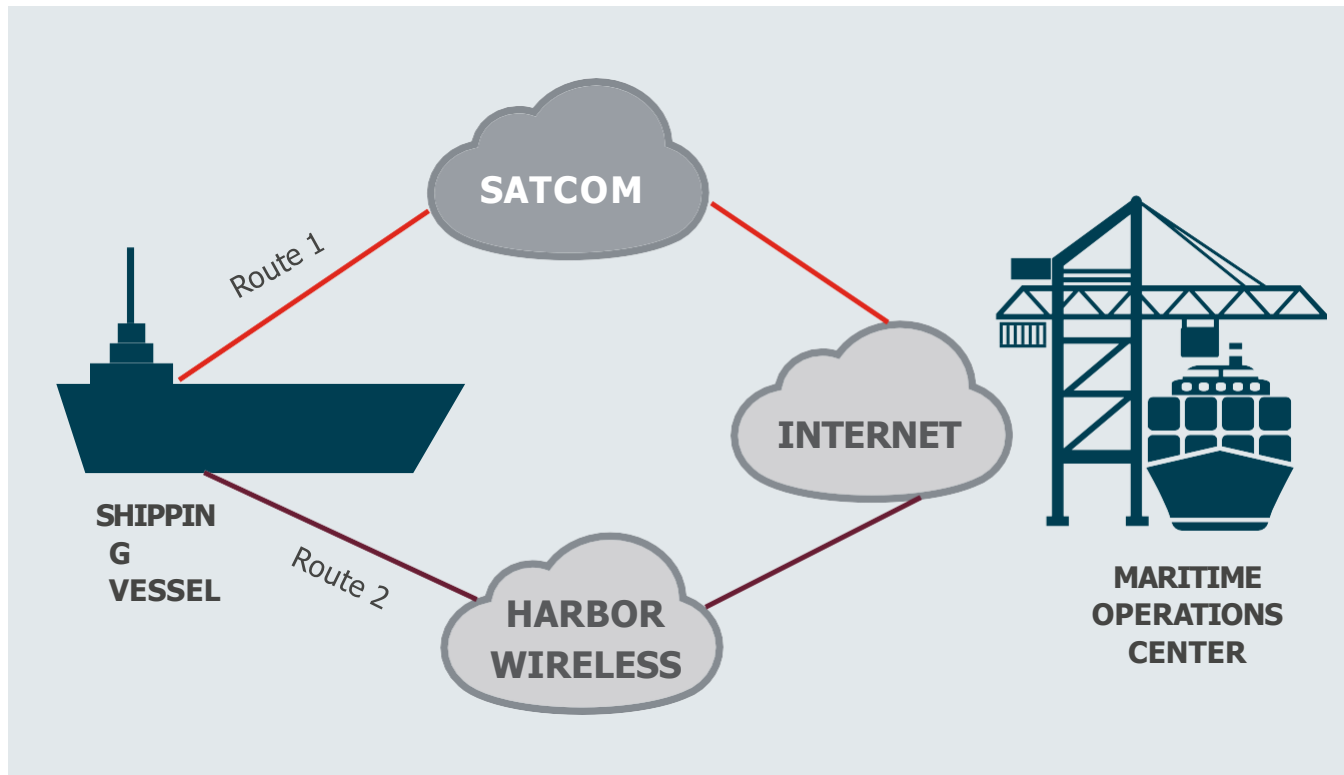
Secure SD-WAN Solution Highlights

- Simplify Deployment with Zero-Touch Provisioning
- Optimize Application Performance
- Reduce SATCOM Costs
- Increase Network Agility and Flexibility with Connectivity Optimization
- Reduce Business Critical Applications & Network Downtime