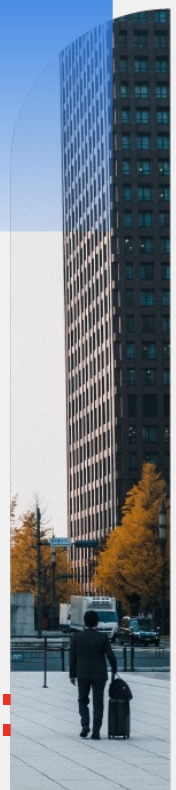
# Moving your fleet on safe and secure seas

Bill Nikolopoulos

Systems Engineering Manager Greece, Hungary and Cyprus



# Elephant in the room !!!

- Maritime cyber risk
- GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
  - IMO has issued MSC-FAL.1-Circ.3-Rev.2 *Guidelines on maritime cyber risk management.*
- Started in 2017 –upd 2022
- Guidelines on Cyber Security on board Ships issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss.

# The Guidelines on Cyber Security Onboard Ships Version 4 (short version)

- Cyber incidents can arise as the result of eg:
  - a cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (**ECDIS**)
  - an unintended system failure occurring during software maintenance and patching, for example through the use of an **infected USB drive** to complete the maintenance
  - loss of or manipulation of external sensor data, critical for the operation of a ship. This includes but is not limited to Global Navigation Satellite Systems (**GNSS**), of which the Global Positioning System (**GPS**) is the most frequently used.
  - failure of a system due to software crashes and/or “bugs”
  - crew interaction with **phishing** attempts, which is the most common attack vector by threat actors, which could lead to the loss of sensitive data and the **introduction of malware to shipboard systems**

# The Guidelines on Cyber Security Onboard Ships Version 4

- The maritime industry has a range of characteristics that affect its vulnerability to cyber incidents.
- These include:
  - involvement of multiple stakeholders in the operation and chartering of a ship potentially resulting in lack of accountability for the IT and OT system infrastructure and ship's networks
  - **use of legacy IT and OT systems** that are no longer supported and/or that rely on obsolete operating systems
  - use of **OT systems that cannot be patched or run anti-virus due to type approval issues**
  - ships that **interface online** with shoreside parties and other parts of the global supply chain
  - the sharing of business critical, data sensitive and commercially sensitive information with shorebased service providers, including marine terminals and stevedores and also, where applicable, public authorities

# The Guidelines on Cyber Security Onboard Ships Version 4

- the availability and use of computer controlled critical systems, which may not have the latest patches installed or be properly secured, for the ship's safety and for environmental protection
- a **cyber risk management culture** that still has potential for improvement, eg through more formalised training, exercises and clarified roles and responsibilities
- frequently the automation system comprises of **multiple sub-systems from numerous vendors** that are integrated by shipyards with minimal regard to cyber issues

# The Industry Agrees…

## IT / OT Convergence

“OT environments that were traditionally separated are no longer completely isolated. They now have direct connections for business, OEMs and other third parties.”

Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework published 17 June 2021

## Long Lifespan

“The automation hardware in a process automation system is often capable of running 20 to 30 years.”

Automation’s Life Cycle Management of Processing Automation Control Systems, published April 2021

## Incidents Underreported

“15% of survey respondents have experienced a security incident last year that crippled operational or mission-critical systems.”

Gartner, Emerging Technologies: Critical Insights for Operational Technology Security published November 10, 2021

## Compromises in IT drive ICS/OT incidents

“Survey participants cite a compromise in IT allowing threats into the ICS/OT control networks as the highest-ranking threat vectors involved in control system incidents.”

SANS 2022 Survey: OT/ICS Cybersecurity, published October 2022

## Mixing legacy and modern tech

“Technical integration of legacy and aging OT technology with modern IT systems is the biggest challenge facing securing OT technology and process.”

SANS 2022 Survey: OT/ICS Cybersecurity, published October 2022

## Ransomware is the highest concern

“Ransomware, extortion, or other financially motivated crimes rank as number one threat vector of concern.”

SANS 2022 Survey: OT/ICS Cybersecurity, published October 2022

# Where do we stand today ?

- Vessel setup
  - Vendor A provides the connectivity
  - Vendor B provides the switching/wireless
  - Vendor C provides the crew internet / cards
  - Vendor D provides the endpoint protection
  - Vendor E OT/IOT
  - Vendor ….

# Where do we stand today ?

- On-shore setup
  - Vendor A provides the connectivity + NGFW/UTM/NGTP protection
  - Vendor B provides the switching/wireless
  - Vendor C provides the SIEM/SOAR
  - Vendor D provides the secure email
  - Vendor E provides the cloud security
  - Vendor …

# Cybersecurity Market and Industry Drivers

## Driving Infrastructure Evolution

How we interact with customers, suppliers, infrastructure, and employees is changing

**Work from Anywhere**

**Digital Acceleration**

**Application Journey**

**Operational Technology Connectivity**

## Evolving Threat Landscape

Cybercriminals are adopting APT-like tactics to develop and scale attacks faster than ever

**Cloud**

*Kaseya VSA*

**Nation Sponsored**

*Hermetic Wiper*

**Ransom as a Service**

*REvil*

**Growing Attack Surface**

*SolarWinds | Log4j*

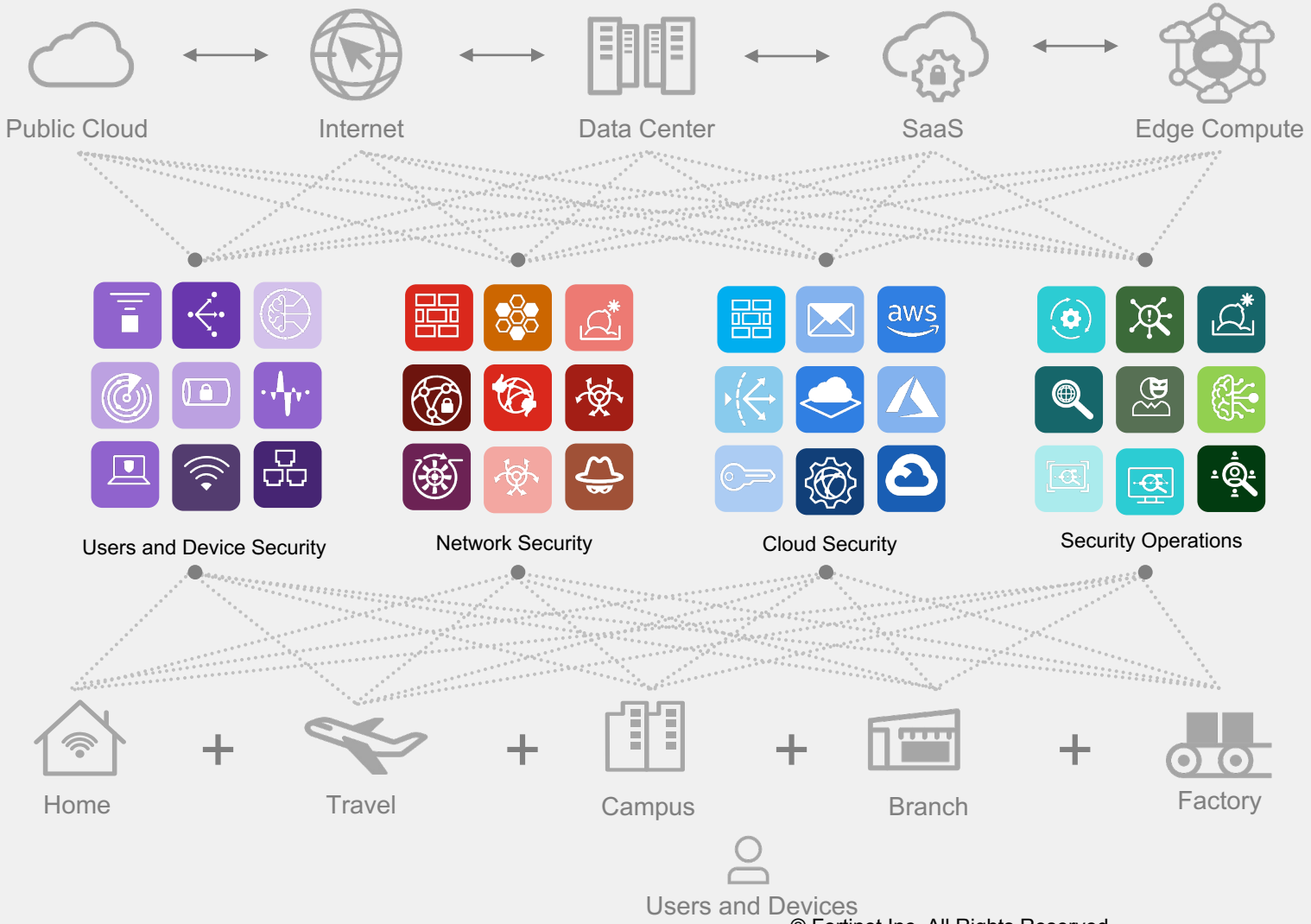
**AI-enabled**

*Swarmbot*

**OT**

*Wipers | Colonial Pipeline*

# Complexity is Slowing Digital Initiatives




## Today's Challenges

- Applications are distributed
- Users are working from anywhere
- More devices are attaching to applications
- Too many IT and security stacks
- Too many vendors
- Cybersecurity skills shortage

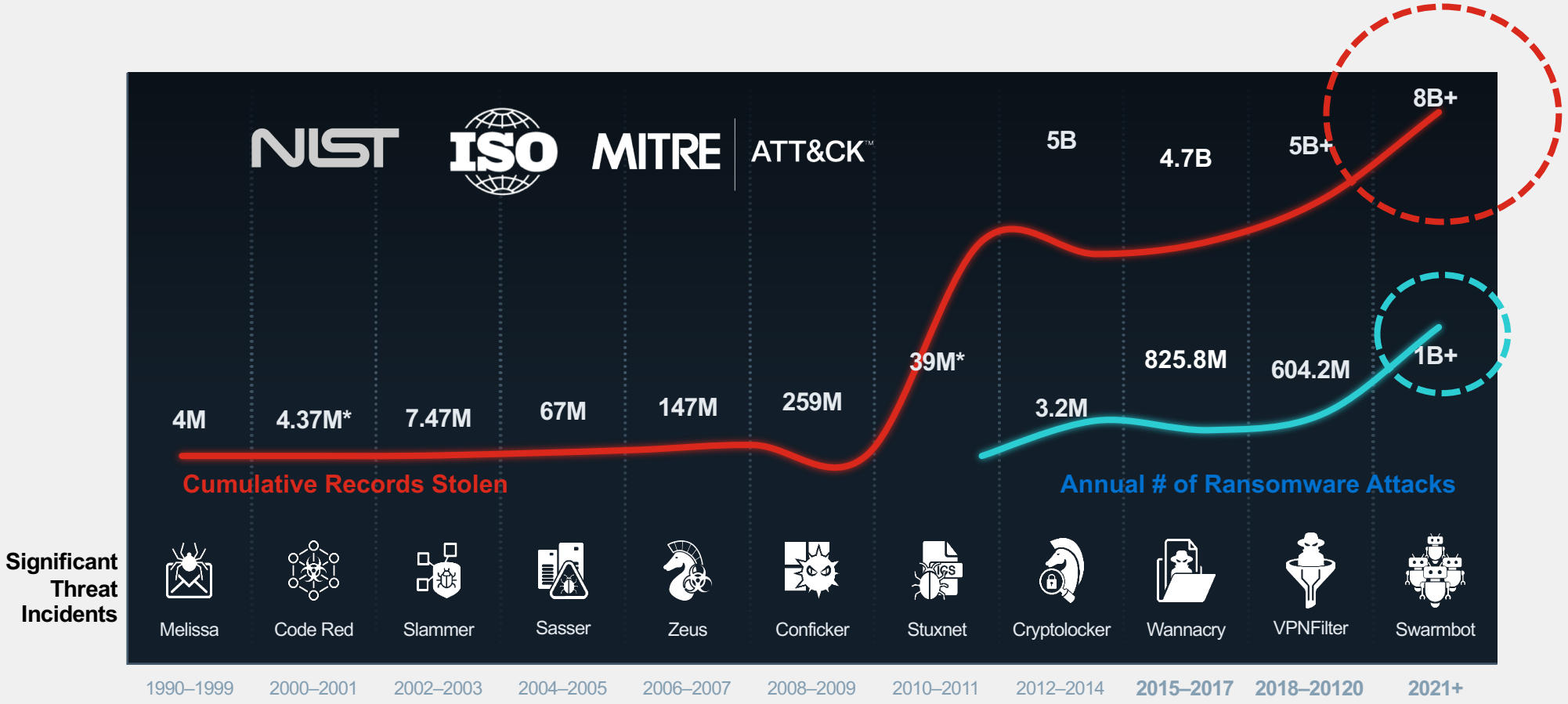
*“There are only two types of companies: Those that have been hacked and those that will be hacked.”*

*-Robert Mueller*

*“There are three types of companies: Those that have been hacked, those that will be hacked and those that are already hacked and they don't know about it..”*

# Advanced Threats Continued to Adapt

## Both in Volume and Sophistication




Protect

Detect

Respond

*many undisclosed | Record Stolen Reference—Breach Level Index | Ransomware stats—Statista

# Attack kill chain

MITRE
Pre-ATT&CK™

Advanced Persistent Cybercrime

MITRE
ATT&CK™

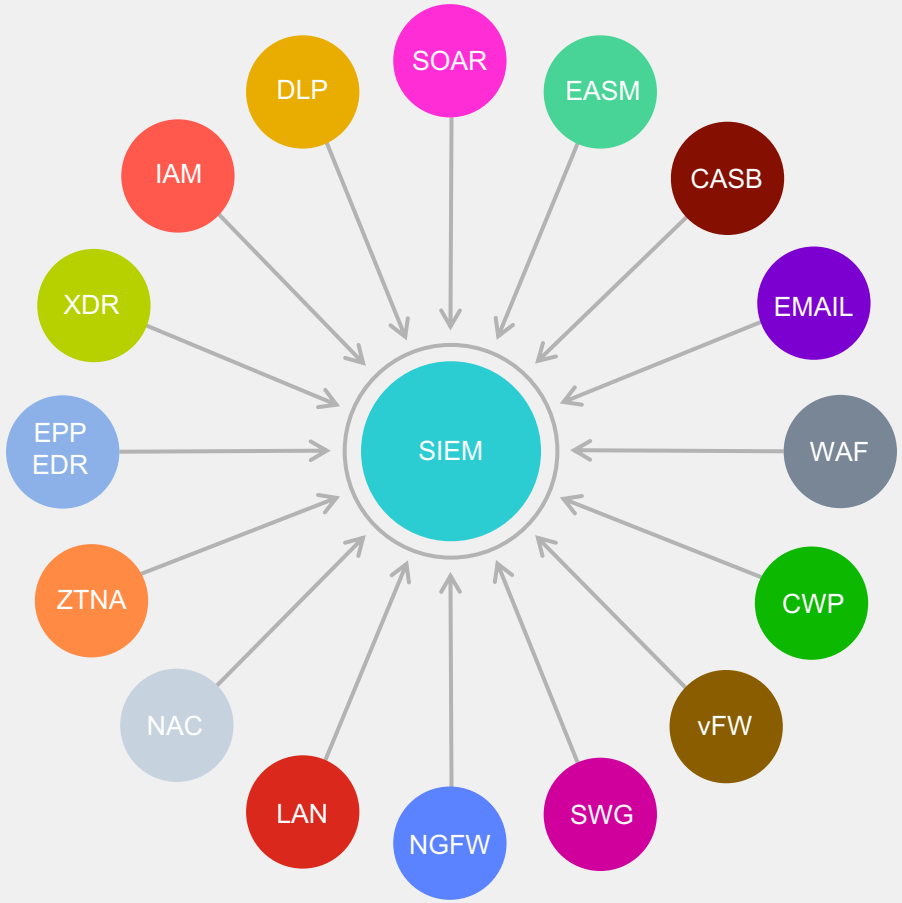
Weaponization of AI

| Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command & Control | Action on Objectives |
|---|---|---|---|---|---|---|
| Detect earliest stage reconnaissance | Identify zero-day threats | Block delivery of weaponized files | Shield vulnerabilities ahead of patches | Prevent installation, execution, encryption | Detect DNS and C2 traffic | Monitor and respond |

# Consolidation of Security Point Product Vendors

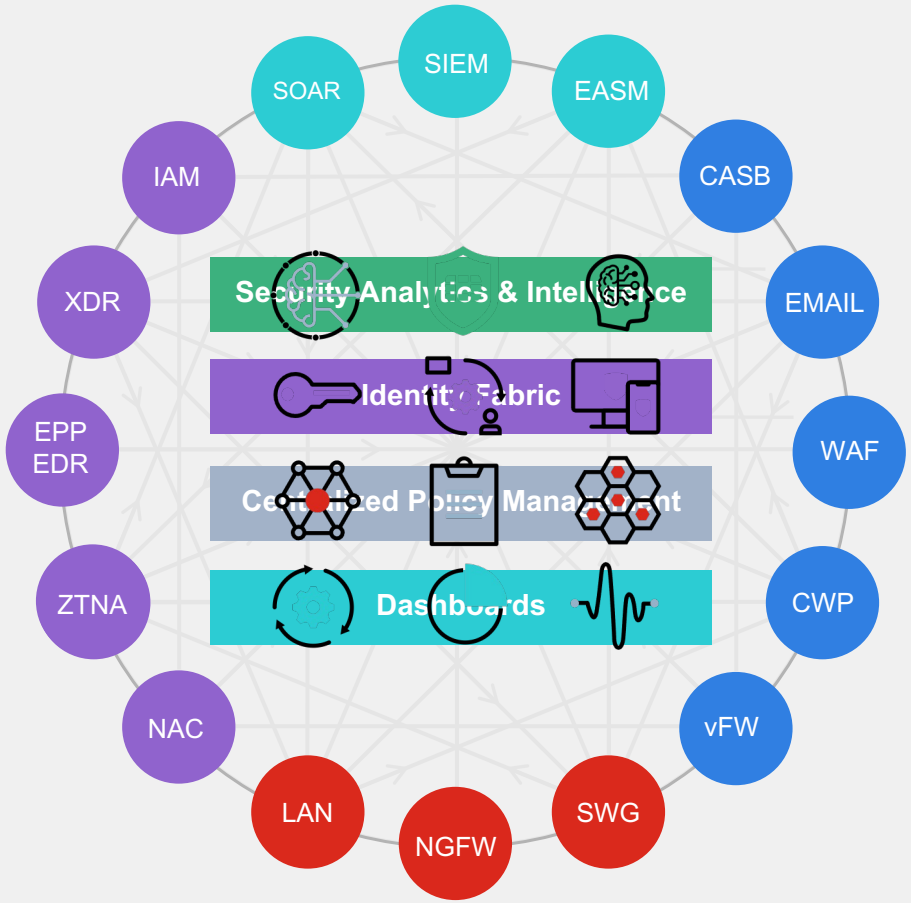
Gartner® Cybersecurity Mesh Architecture (CSMA)

## Cybersecurity Point Products




20 Vendors

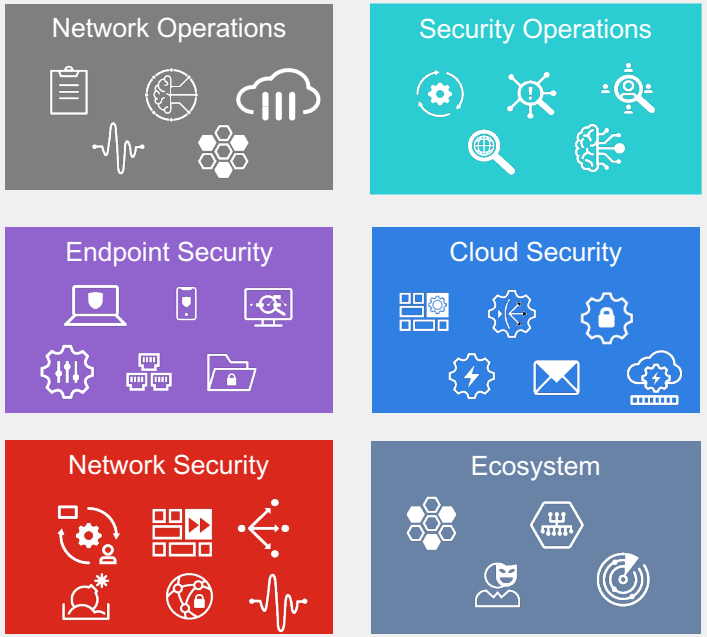
## Cybersecurity Platform Approach



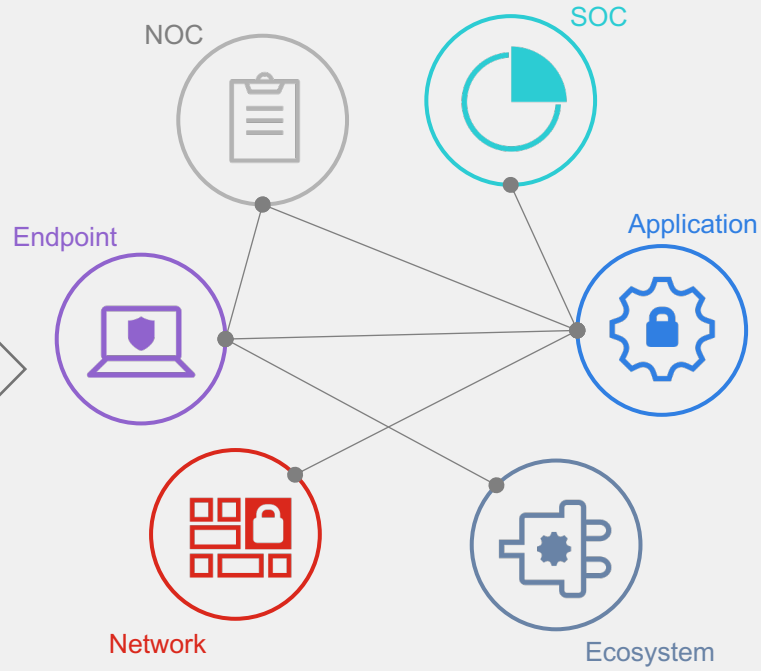

4-6 Platforms

# Cybersecurity Platform Journey

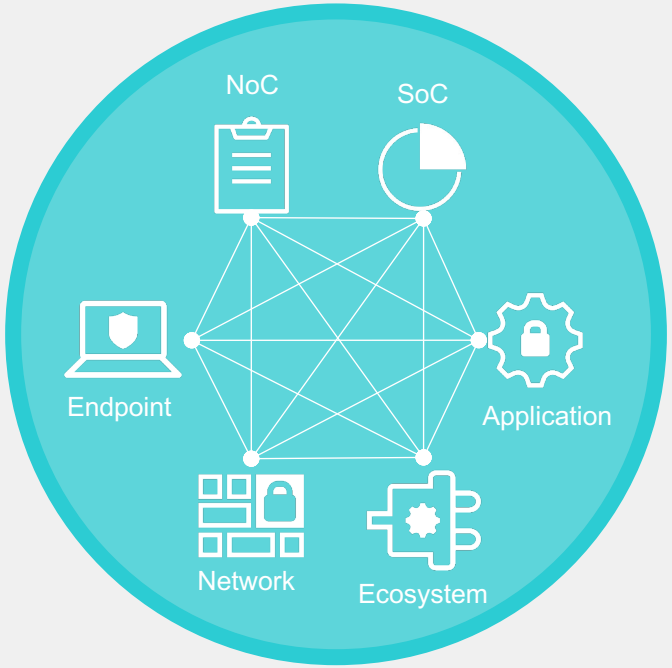

## 30+ Vendors




## 10 Vendors




## 2-3 Platforms




**Your Journey to SOC Automation Maturity**

# Fortinet journey

- One-liner Fortinet Security Fabric **PLATFORM**

# Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

## Secure Networking

**FortiGate**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

**FortiGate SD-WAN**
Application-centric, scalable, and Secure SD-WAN with NGFW

**FortiExtender**
Extend scalable and resilient LTE and LAN connectivity

**FortiAP**
Protected LAN Edge deployments with wireless connectivity

**FortiSwitch**
Deliver security, performance, and manageable access to data

**Linksys HomeWRK**
Secure Work-from-Home solution for remote and hybrid workers

**FortiNAC**
Visibility, access control and automated responses for all networked devices

**FortiProxy**
Enforce internet, compliance and granular application control

**FortiIsolator**
Maintain an "air-gap" between browser and web content

## Cloud Security

**FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

**FortiDDOS**
Machine-learning quickly inspects traffic at layers 3, 4, and 7

**FortiCNP**
Manage risk and compliance through multi-cloud infrastructures

**FortiDevSec**
Continuous application security testing in CI/CD pipelines

**FortiWeb**
Prevent web application attacks against critical web assets

**FortiADC**
Application-aware intelligence for distribution of application traffic

**FortiGSLB Cloud**
Ensure business continuity during Unexpected network downtime

**FortiMail**
Secure mail getaway to protect against SPAM and virus attacks

**FortiCASB**
Prevent misconfigurations of SaaS applications and meet compliance

## Zero Trust Access

**FortiSASE**
Enforce dynamic network access control and network segmentation

**ZTNA Agent**
Remote access, application access, and risk reduction

**FortiAuthenticator**
Identify users wherever they are and enforce strong authentication

**FortiToken**
One-time password application with push notification

**FortiClient Fabric Agent**
IPSec and SSL VPN tunnel, endpoint telemetry and more

**FortiGuest**
Simplified guest access, BYOD, and policy management

## FortiGuard Threat Intelligence

Powered by FortiGuard Labs


## Fabric Management Center: NOC

**FortiManager**
Centralized management of your Fortinet security infrastructure

**FortiGate Cloud**
Saas w/ zero touch deployment, configuration, and management

**FortiMonitor**
Analysis tool to provide NOC and SOC monitoring capabilities

**FortiAIOps**
Network inspection to rapidly analyze, enable, and correlate

**FortiExtender Cloud**
Deploy, manage and customize LTE internet access

**FNDN**
Exclusive developer community for access to advanced tools & scripts

## Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

**Fabric Connectors**
Fortinet-developed

**DevOp Tools & Script**
Fortinet & community-driven

**Fabric API Integration**
Partner-led

**Extended Ecosystem**
Threat sharing w/ tech vendors

## Fabric Management Center: SOC

**FortiDeceptor**
Discover active attackers inside with decoy assets

**FortiNDR**
Accelerate mitigation of evolving threats and threat investigation

**FortiEDR**
Automated protection and orchestrated incident response

**FortiSandbox / FortiAI**
Secure virtual runtime environment to expose unknown threats

**FortiAnalyzer**
Correlation, reporting, and log management in Security Fabric

**FortiSIEM**
Integrated security, performance, and availability monitoring

**FortiSOAR**
Automated security operations, analytics, and response

**FortiTester**
Network performance testing and breach attack simulation (BAS)

**SOC-as-a-Service**
Continuous awareness and control of events, alerts, and threats

**Incident Response Service**
Digital forensic analysis, response, containment, and guidance

## Support & Mitigation Services

**FortiCare Essentials***
15% of hardware

**FortiCare Premium***
20% of hardware

**FortiCare Elite****
25% of hardware

**FortiConverter**
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

## Communication and Surveillance

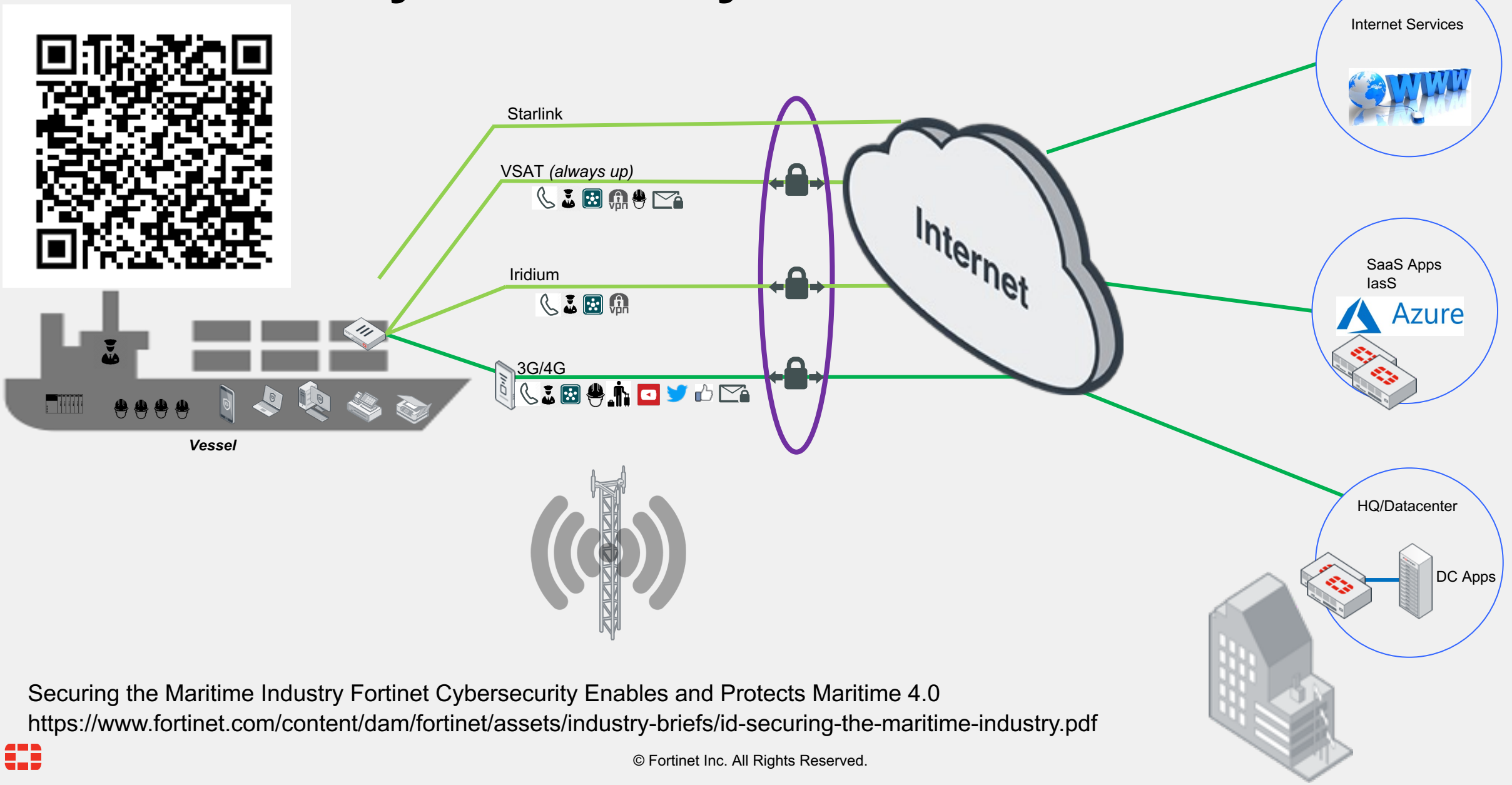
**FortiFone**
Robust IP Phones w/ HD Audio with centralized management

**FortiVoice**
Integrated voice, chat, conferencing management, and fax with centralized

**FortiCamera**
HDTV-quality surveillance cameras for physical safety and security

**FortiRecorder**
High-performance NVR with AI-powered video management software

# The Fortinet Cyber Security Solution

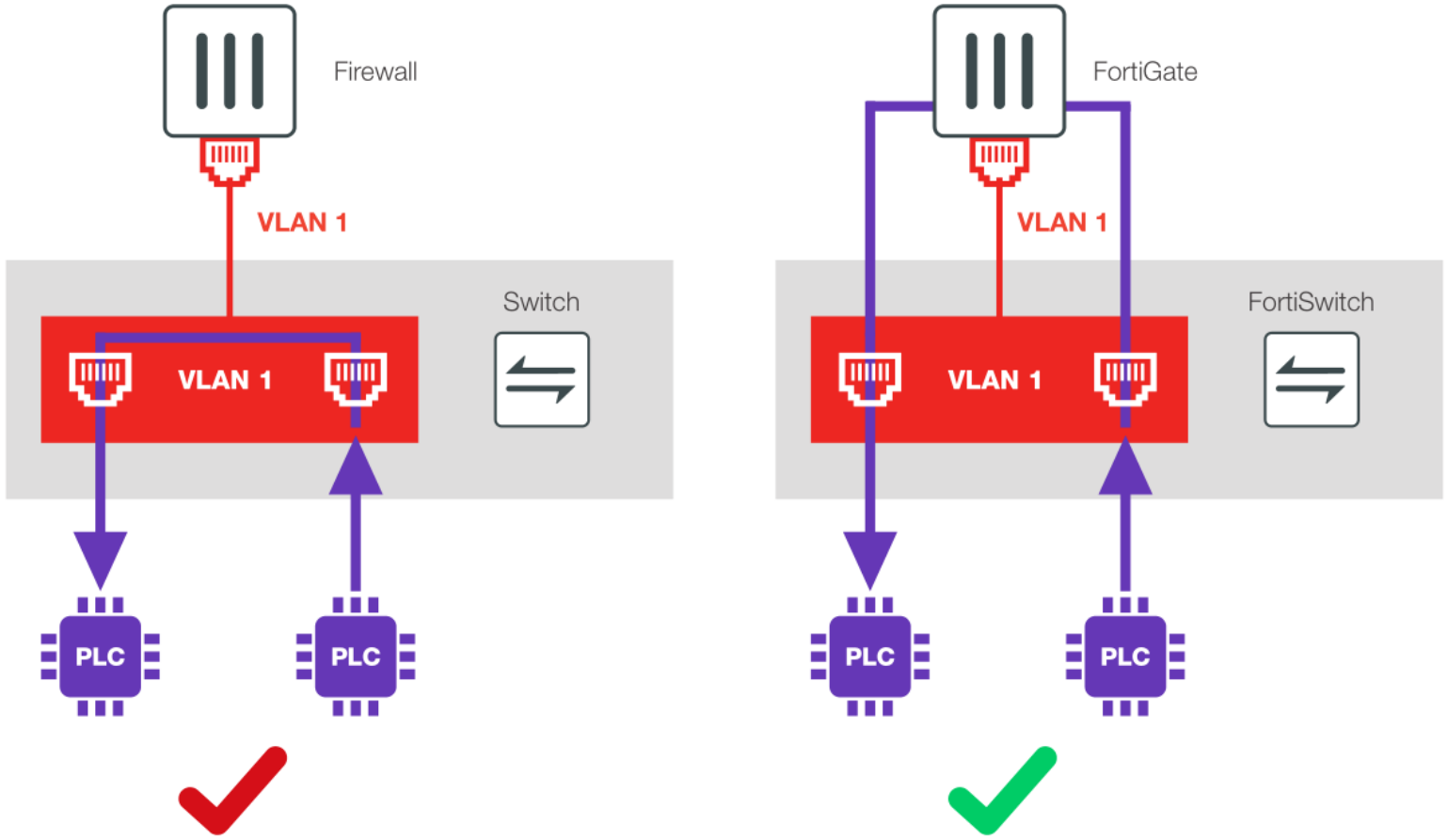



Securing the Maritime Industry Fortinet Cybersecurity Enables and Protects Maritime 4.0
https://www.fortinet.com/content/dam/fortinet/assets/industry-briefs/id-securing-the-maritime-industry.pdf

# OT Use Case

- Customer story => I don’t know where to start…
- Our answer:
  - Let’s keep it simple
  - Fortigate devices are just an enabler for the **Fortinet Security Fabric**

# Microsegmentation




Normal VLAN routing vs. microsegmentation using Fortinet FortiSwitch and FortiGate.

# Real use case


# Ship Propulsion System protected by Fortinet


FORTINET®