NOZOMI NETWORKS

Digital Ship

Monitoring onboard networks

NOZOMI NETWORKS

NOZOMI NETWORKS

Digital Ship

Market Challenges

Market Forces Driving Change

Digital Transformation

- New technologies, new use cases in every industry

IT/OT Convergence

- Integrated teams and workflows need a single view

Internet of Everything

- Juniper Research: 83 billion IoT connections by 2024; 70% in Industrial sector

Threat & Risk Management

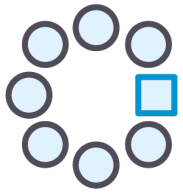
- Frequency and cost of targeted attacks continue to increase

5G is accelerating digital transformation across all sectors – everyone is connected to everything, and new use cases are speeding OT, IoT and IT convergence.

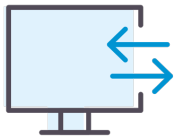
Andrea Carcano, Co-founder and CPO, Nozomi Networks

How OT Security Differs from IT Security

Safety and Reliability of critical systems that operate 24/7/365 and involve processes with significant safety risks.



Heterogeneous/Legacy Systems Industrial networks include diverse assets, and often consist of multiple connected architectures.



Industrial Protocols are often unknown in the IT world, and that are inherently insecure.

Volume of IoT/OT Devices will grow to billions worldwide vs millions in IT.

OT Systems Evolution

Fully Air-Gapped OT System

OT System Partially Connected to Each Other

"Retrofitted" Cyber-Physical System Through IT/OT Convergence

Newly Designed/ Engineered Cyber-Physical System

More Isolation → More Connectivity

Examples of Traditional OT Systems

- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)
- Programmable Logic Control (PLC)
- Process Control Networks (PCN) – Including Safety Instrumented Systems (SIS), Engineer Workstation and Human Machine Interface (HMI)
- Distributed Control Systems (DCS)
- Computer Numerical Control (CNC)

Examples of OT-Related Cyber-Physical Systems

- Industrial Robots
- Virtual Reality Manufacturing Simulation Systems
- Self-Optimizing Press-Bending and Roll-Forming Machine
- Adaptable Production Systems
- Energy-Efficient Intralogistics Systems
- Connected 3D Printers
- Smart Grids

The High Cost of a Cybersecurity Incident

1.7M USD

Average estimated cost of cyberattack

> Cyberattacks on critical infrastructure have become the new normal and are one of the top five global risks."
>
> **World Economic Forum**
> **Global Risk Report, 2020**

	Organization	Issue/Attack	Cost (USD)
2020	Cognizant	Maze Ransomware	70m
	Honda	COVID-related Ransomware	Unknown
2019	Norsk Hydro	LockerGoga Ransomware	70m
	Duke Energy	Compliance Violation	10m
2018	Saudi Petrochem	Triton	Unknown
	UK NHS	WannaCry	100m
2017	Merck	NotPetya	870m
	FedEx (TNT Express)	NotPetya	400m
	Maersk	NotPetya	300m
	Mondelēz	NotPetya	188m
2016	Ukrenergo	Industroyer/Crashoverride	Outage
2012	Saudi Aramco	Shamoon	1 Billion

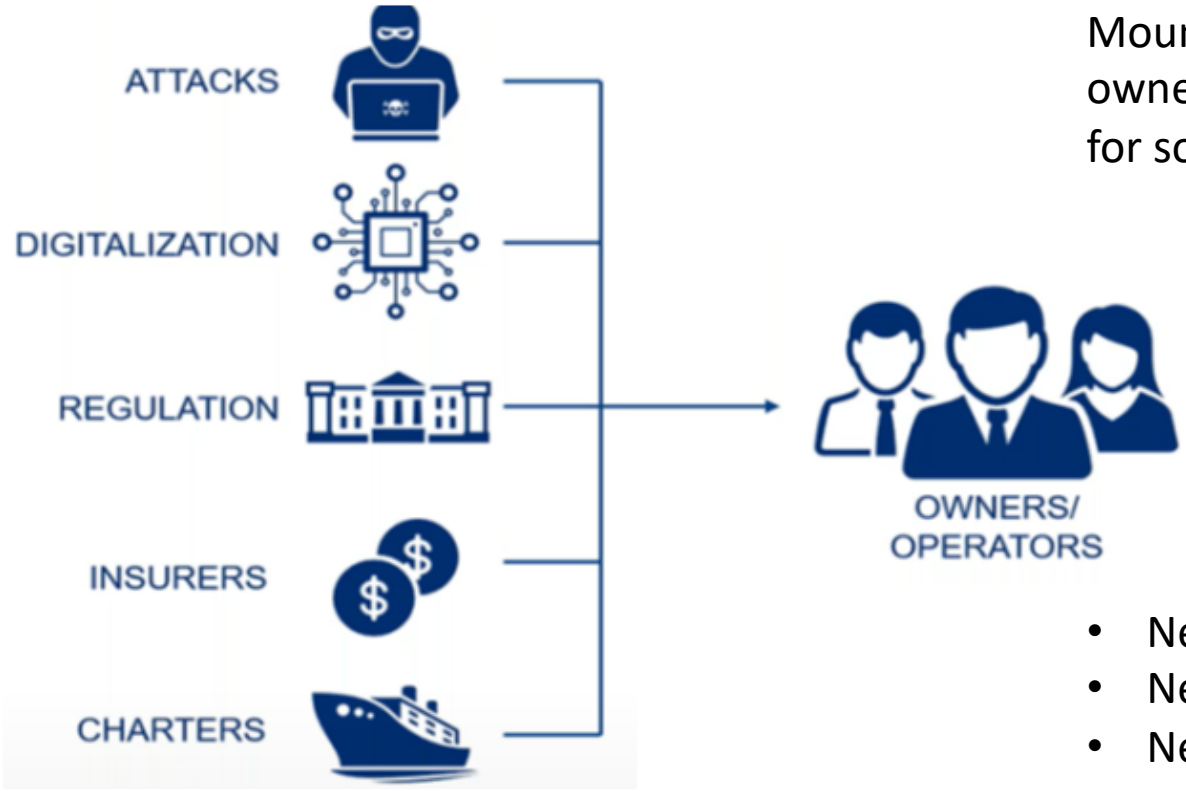
Sources: Wired, Wall Street Journal, UK Telegraph, Threatpost, Forbes

NOZOMI NETWORKS

Digital Ship

Maritime Challenges

Demand for Comprehensive Cybersecurity Solutions in Maritime



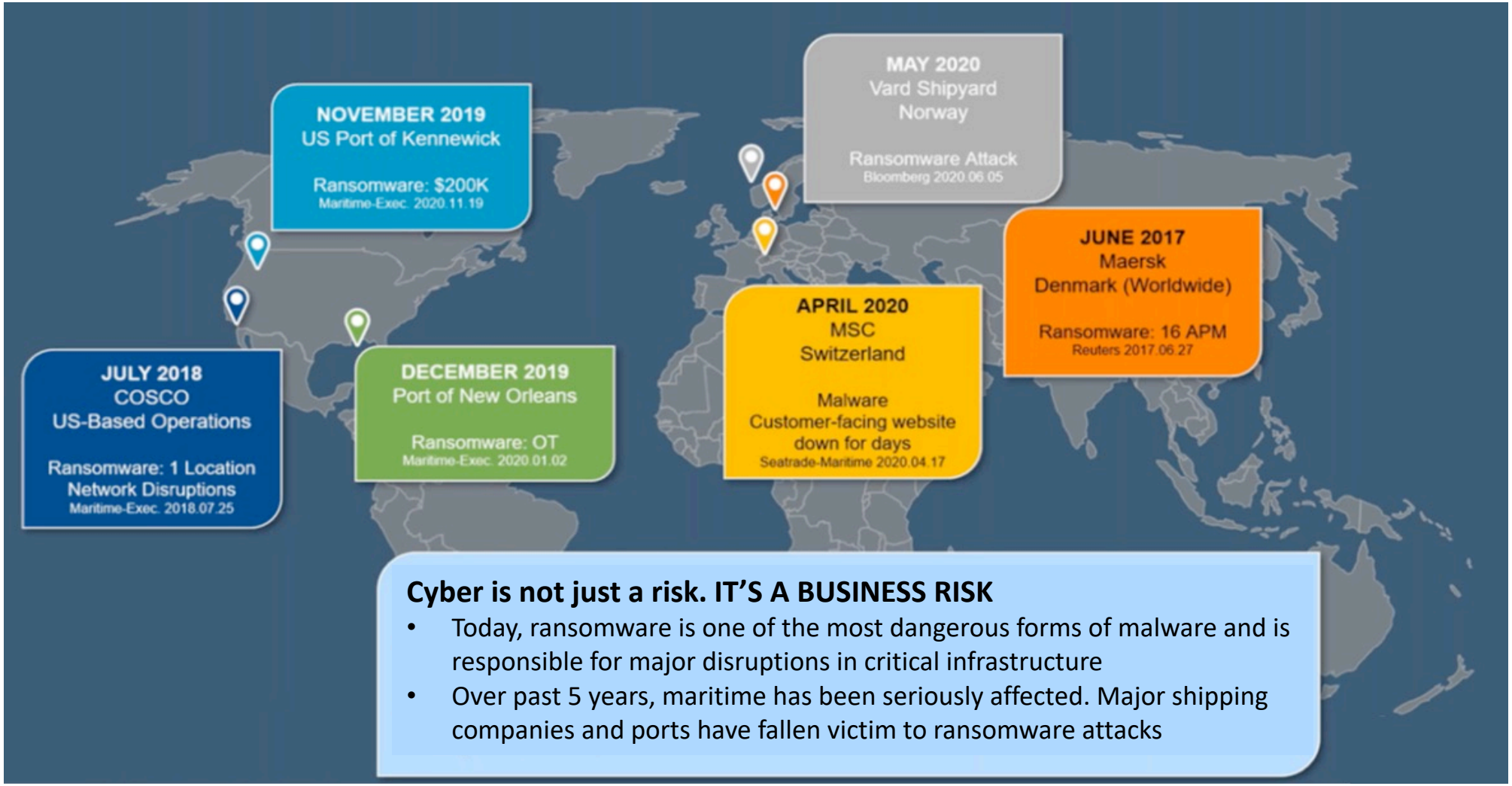
Mounting pressure on owners is creating a demand for solutions

- Need domain expertise
- Need IT/OT solutions
- Need comprehensive solutions

Rules and Regulations

- **ISM Code (International Safety Management)** : *Assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards*
- ***IMO*** *Resolution MSC.428 (98) on cyber risk management – from January 2021*
- **USA Cost Guards**
  To impose Cyber Security to vessel going to USA
- ***ENISA :*** *European Union Agency for Cybersecurity : Guideline for Navigating Cyber Risk – 17th December 2020*
- **National and regional Cyber security and Data Privacy laws and regulation**: *E.g. US CG Cyber Security Profiles and CG-5P Policy Letter 08-16, EU GDPR, EU critical infrastructure – Directive(EU) 2016/1148, UK Code of Practice, etc.*
- **Cyber security exclusion clause in insurance**: (Clause 380) exclude coverage of cyber security incidents.
- ***OCIMF (Oil Companies International Marine Forum)*** *: Tanker Management and Self Assessment (TMSA) – As January 2018 / In Evaluation for dry-cargo ships*

Business Risk for Maritime Industry



Cyber is not just a risk. IT'S A BUSINESS RISK

- Today, ransomware is one of the most dangerous forms of malware and is responsible for major disruptions in critical infrastructure
- Over past 5 years, maritime has been seriously affected. Major shipping companies and ports have fallen victim to ransomware attacks

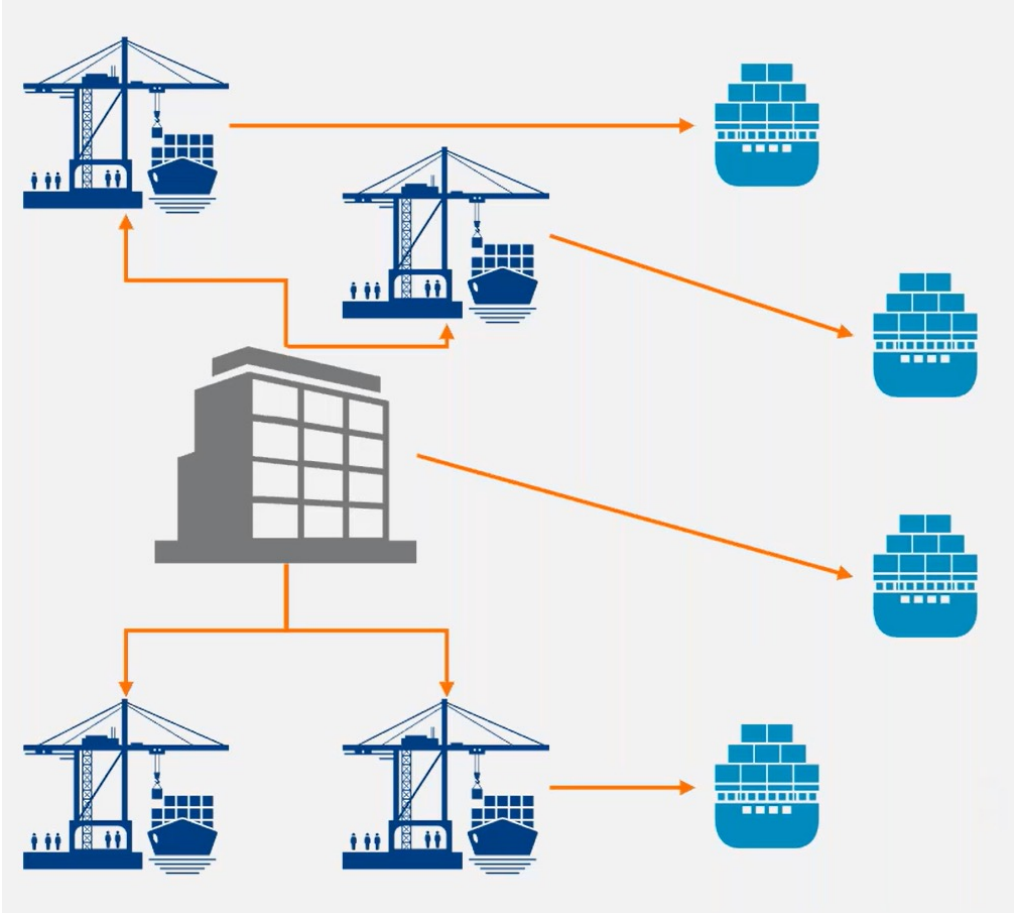
Shipping Ransomware Attack

A major maritime shipping company experienced a ransomware attack affecting 17 of its ports.

- The attack prevented port personnel from accessing operations data and moving cargo for 2 days.
- It took 2 weeks before business was back to normal.
- The event resulted in a 300$ million-dollar loss.

What happened

- It began in a small office in a foreign country that had a network server connected to other offices.
  - The wrong update spread the "*NotPetya*" virus throughout the company.
- The shipping company was not believed to be the intended target.
- The CEO said that they had not taken cybersecurity seriously before the incident, but now they consider cybersecurity as a competitive advantage.

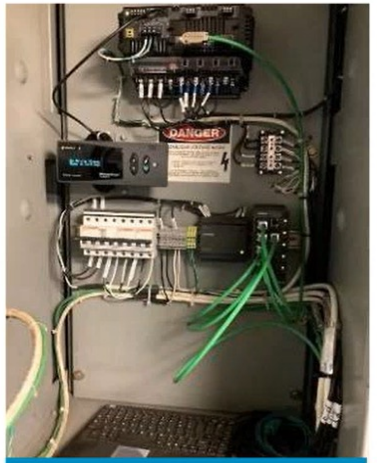


Maritime Operational Technology

Vessel Monitoring System

Relay Control System

Vessel Maneuvering System

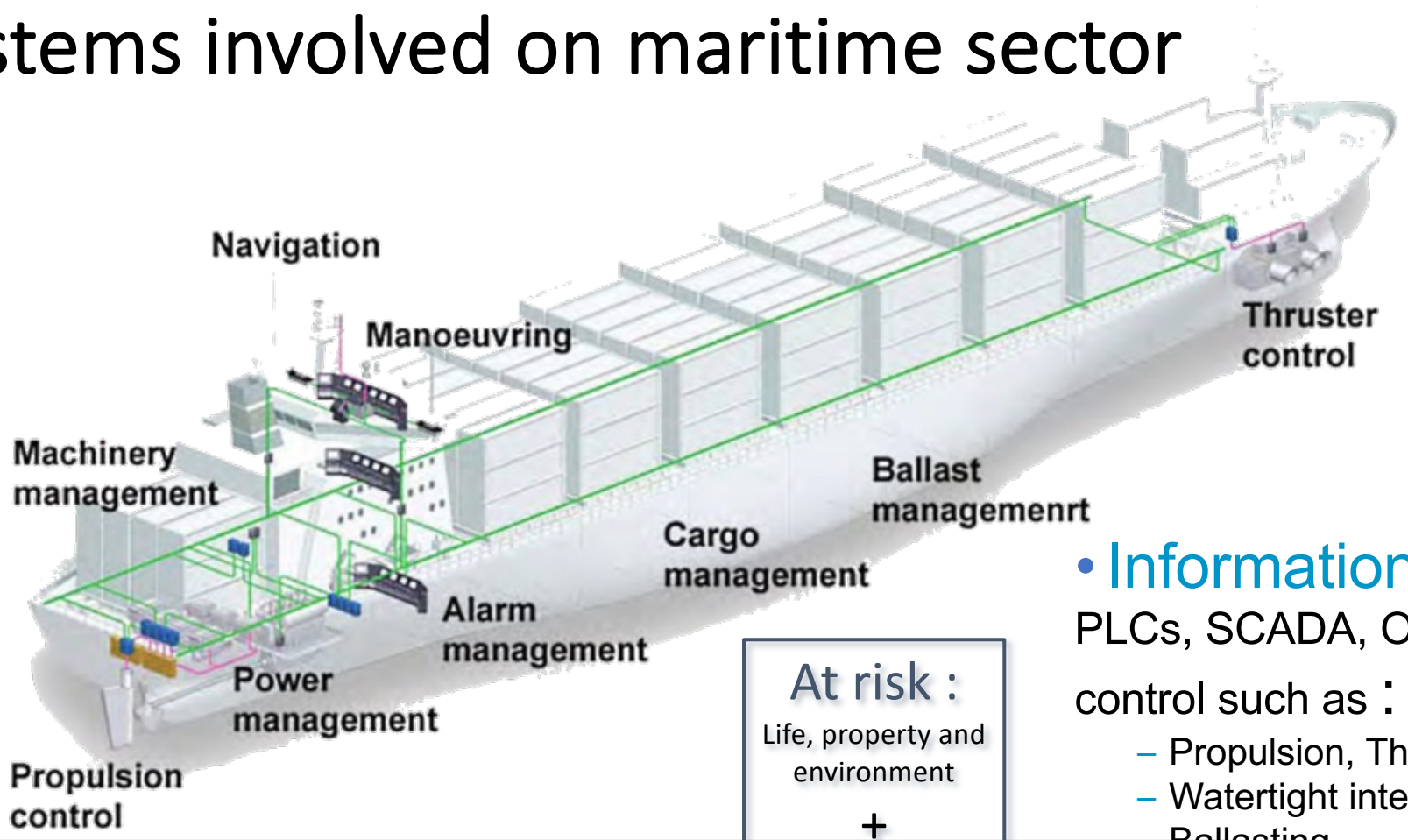


Cargo Monitoring System

Engine Control System

Vessel Maneuvering System

Systems involved on maritime sector



At risk :

Life, property and environment

+

All next

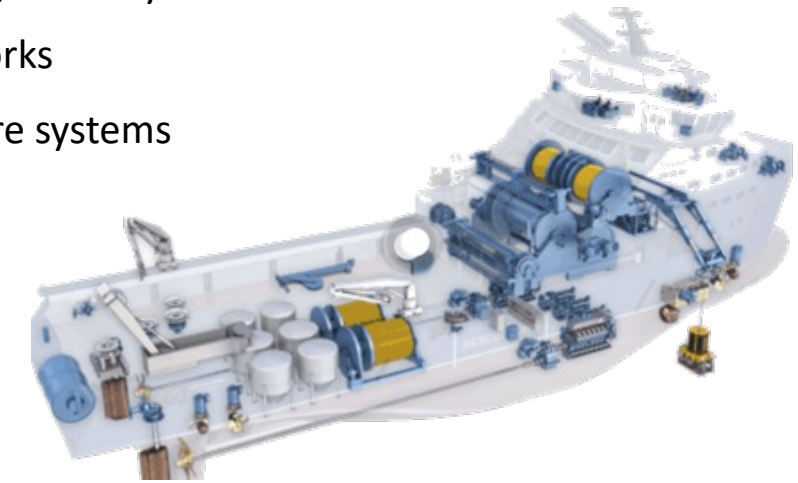
- **Information technology (OT)**

PLCs, SCADA, On-Board measurement and control such as :

- Propulsion, Thrusters and Steering
- Watertight integrity and Fire Detection
- Ballasting
- Power generation and Auxiliary systems
- Navigation and communication (ECDIS, etc.)
- Industrial systems (DP, Drilling, etc.)

IMO (International Maritime Organization) Vulnerable Systems

- Bridge Systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passengers facing public networks
- Administrative and crew welfare systems
- Communication systems



NOZOMI NETWORKS

Digital Ship

The Nozomi Networks Solution

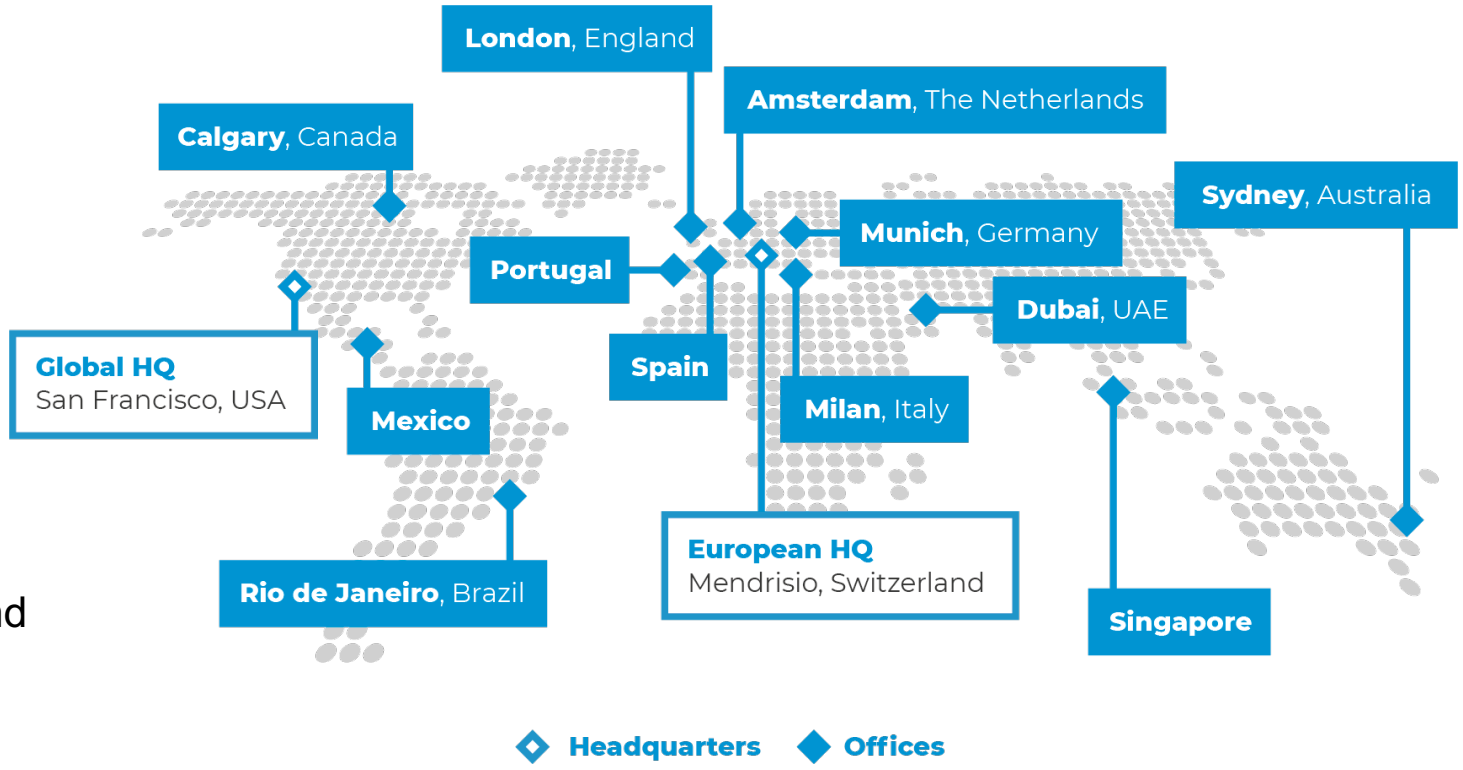
Global Leadership Footprint

Global Customer Base
7.6K Installations

82M Devices Monitored
Across Converged OT/IoT/IT

Scalable Deployments
Across **6 Continents**

Global Expertise
Worldwide Network of Partners and
1,000+ Certified Professionals



Securing the World's Largest Organizations

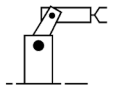
9 of Top 20
Oil & Gas

7 of Top 10
Pharma

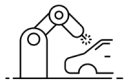
5 of Top 10
Mining

5 of Top 10
Utilities

Chemicals

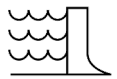


Manufacturing



Automotive

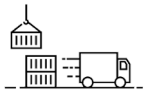
Airports



Water

Building Automation

Food & Retail



Logistics

Smart Cities

Transportation

NOZOMI NETWORKS

2022 Growth

100% Customer **retention**

100% Customer **growth**

83% **win rate** for PoCs

90% of the time, **vulnerabilities/ threats** found within 24 hours of installation

Industry-1st SaaS solution for OT/IoT cybersecurity: **Vantage™**

Industry Leader for *4th* consecutive year in **Gartner Peer Insights Reviews**

Unrivaled Partner Ecosystem adding Honeywell, Telefónica, ABB, AWS, Honeywell, Siemens, Google, Service Now, Yokogawa, and other

Strategic Investments from In-Q-Tel, Telefónica and Forward Investments

Nozomi Networks Key Differentiators

See

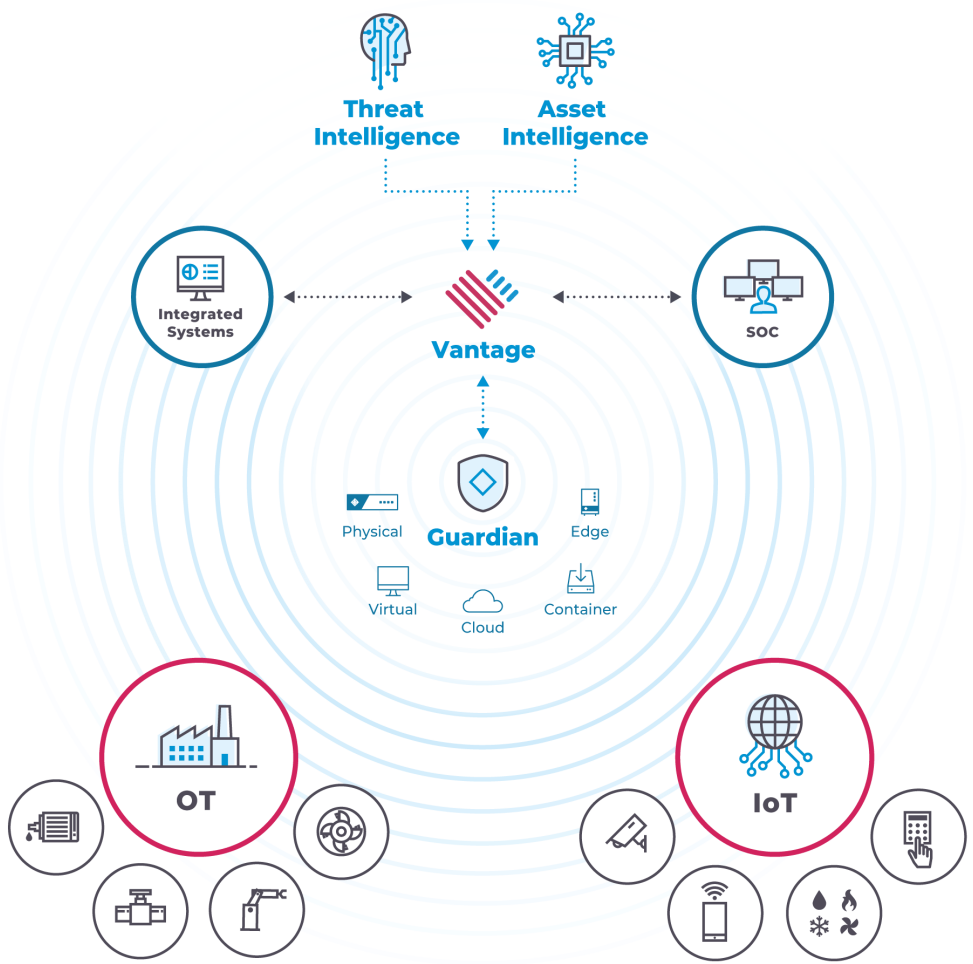
All assets and behaviors on your OT/IoT networks for comprehensive awareness

Detect

Cyber threats, vulnerabilities, risks and anomalies for faster response

Unify

Security, visibility and monitoring across all your assets for improved operational resilience



NOZOMI NETWORKS

Digital Ship

Nozomi Networks Solution Portfolio

CORE SOLUTIONS

- **Vantage**
- **Guardian**
- **Central Management Console**

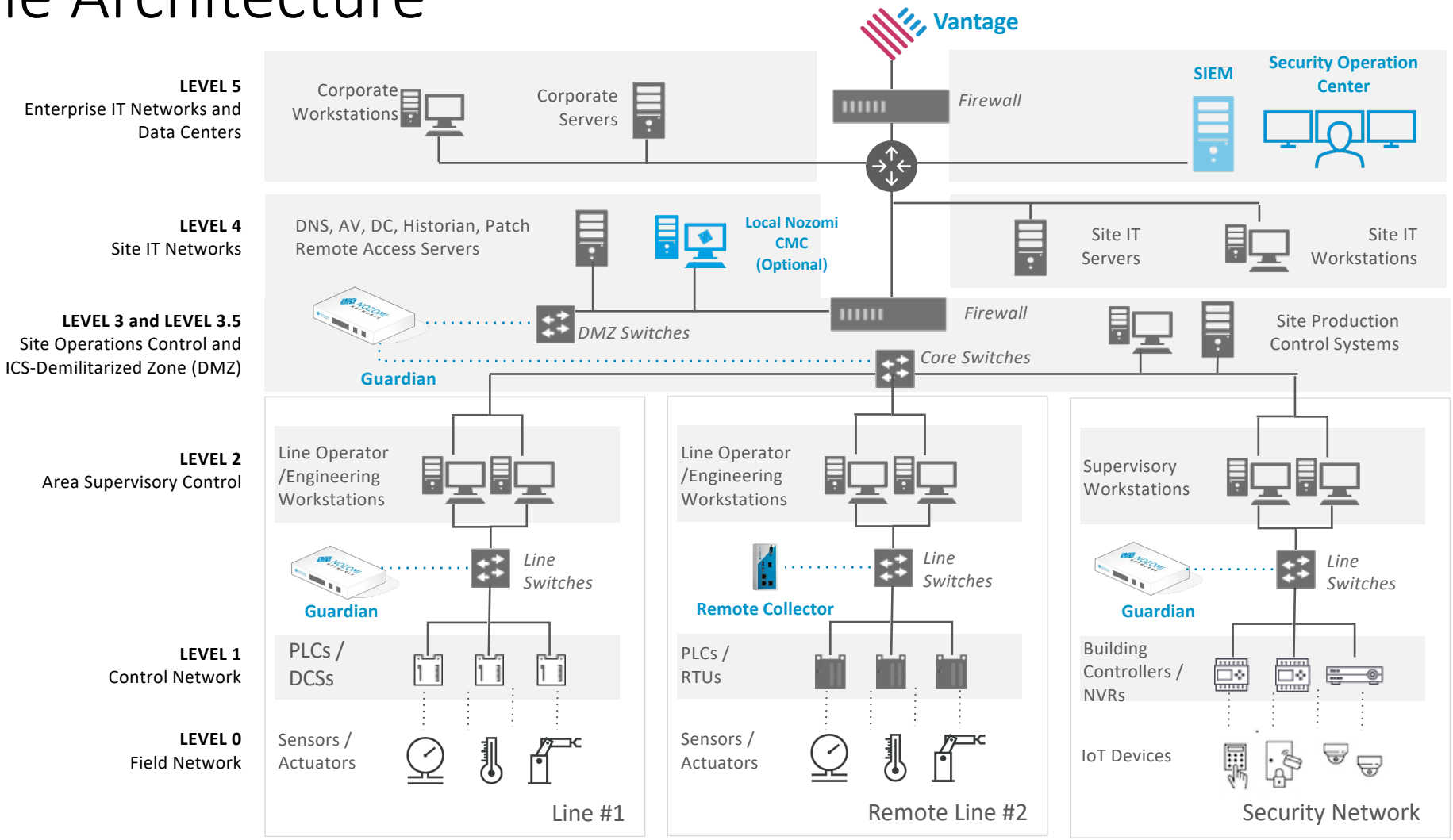
EXTENDED FUNCTIONALITY

- **Smart Polling**
- **Asset Intelligence**
- **Threat Intelligence**
- **Remote Collectors**

SERVICE OFFERINGS

- **Certified Engineer Training**
- **Professional Services**
- **Customer Support**

Sample Architecture



Superior Asset Discovery & Monitoring

Vendor	Rockwell Eng
IP	192.168.0.10
OS	Windows 7 / 2008 R2
Patch Vuln	?

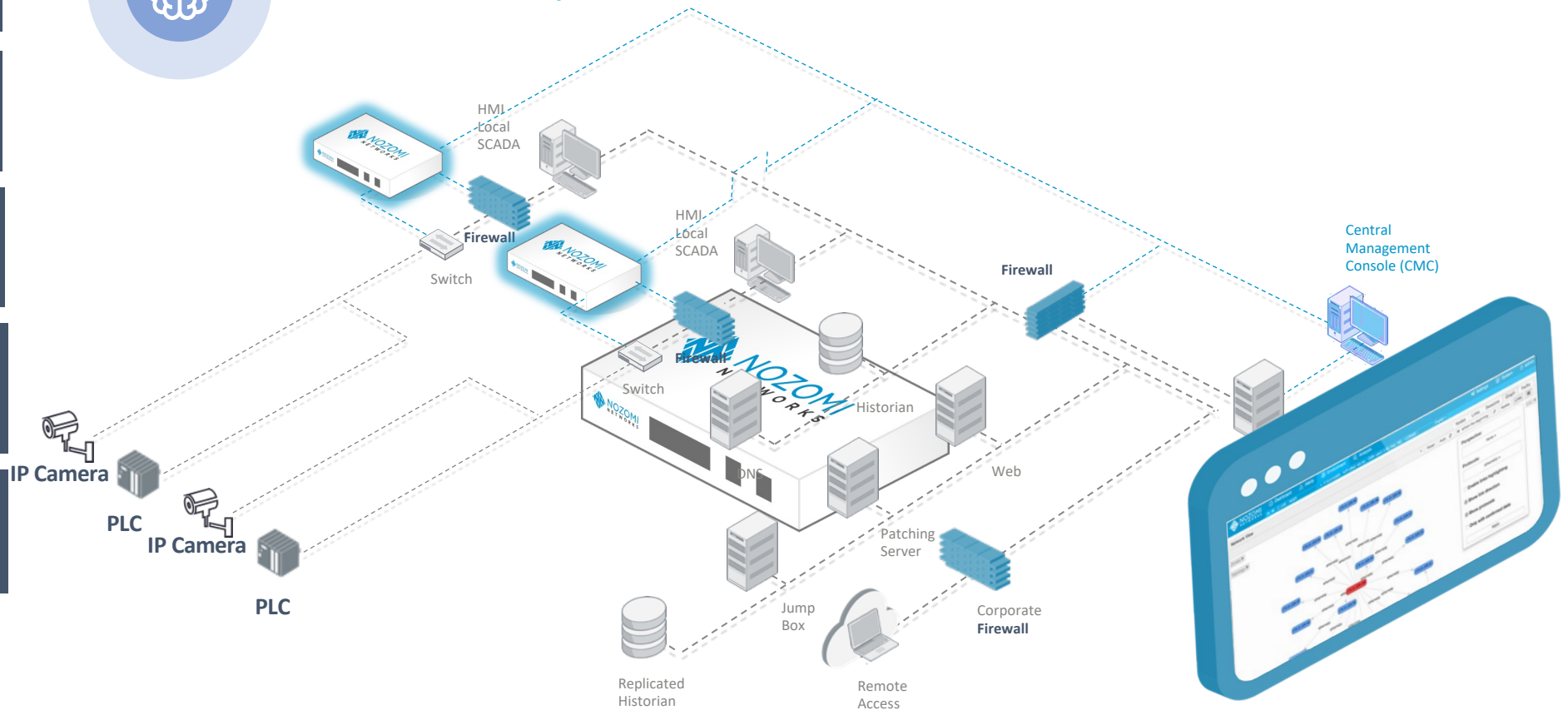
Vendor	Honeywell
IP	192.168.0.251
Firmware	16.020
Module #	0123

Vendor	AXIS
IP	192.168.0.144
Firmware	6.50.2.3
Model #	AXIS Q1615-E

Vendor	Rockwell
IP	192.168.1.80
Firmware	?
Module #	?

Vendor	AXIS
IP	192.168.50.128
Firmware	8.20.1
Model #	Q1615-E Mk II

AI-Enabled
Passive Auto-Discovery



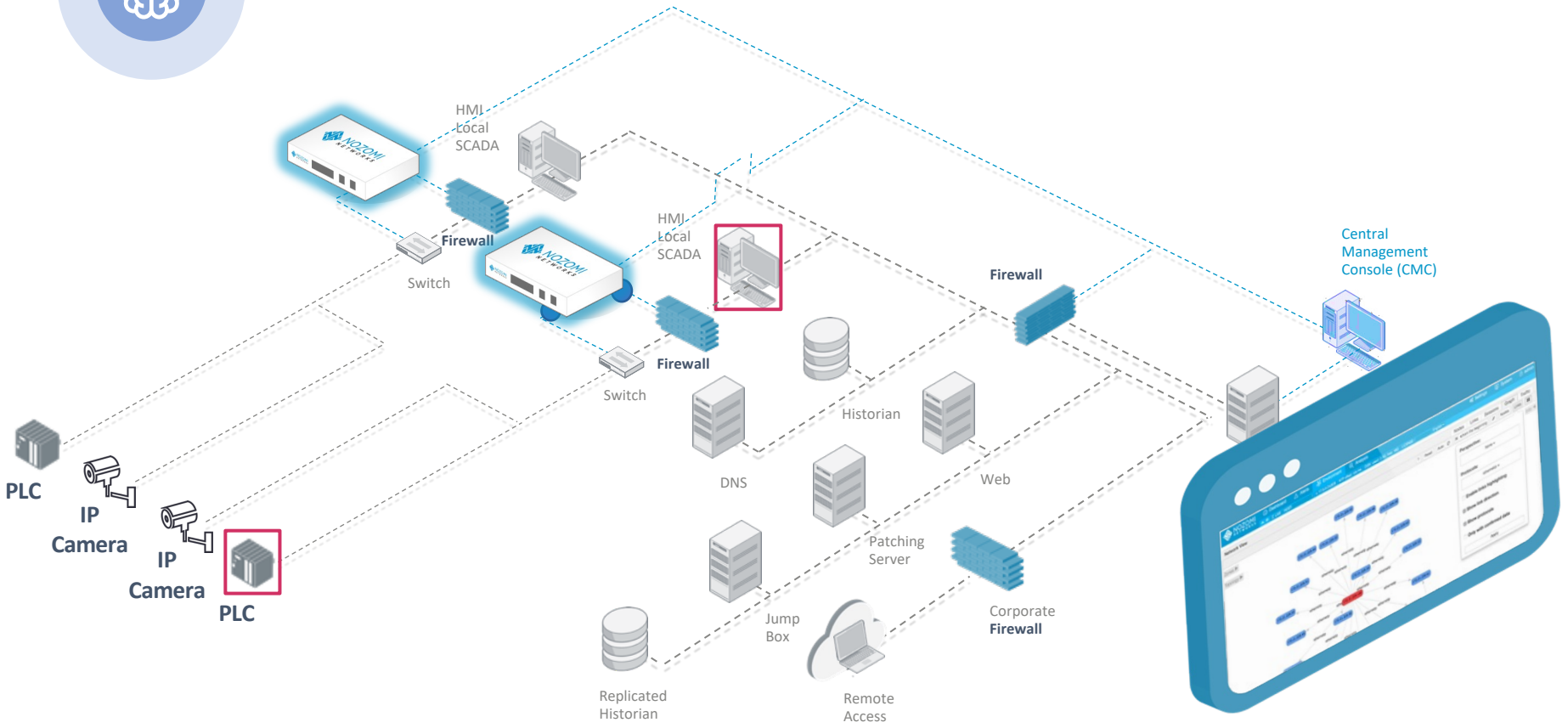
Superior Asset Discovery & Monitoring

Vendor	Rockwell Eng
IP	192.168.0.10
OS	Windows 7 SP1
Patch Vuln	34 missing KBs

Vendor	Rockwell
IP	192.168.1.80
Firmware	16.020
Module #	0173

There is insufficient network data to provide details.

AI-Enabled **Passive Auto-Discovery + Smart Polling**



- Confirms vulnerabilities for faster, more efficient response
- Offers a default configuration, or manual options, for applying Smart Polling to specific devices and network segments only
- Uses native communication protocols, WinRM, WMI, SNMPv2, SNMPv3, SSH, etc. to collect asset data

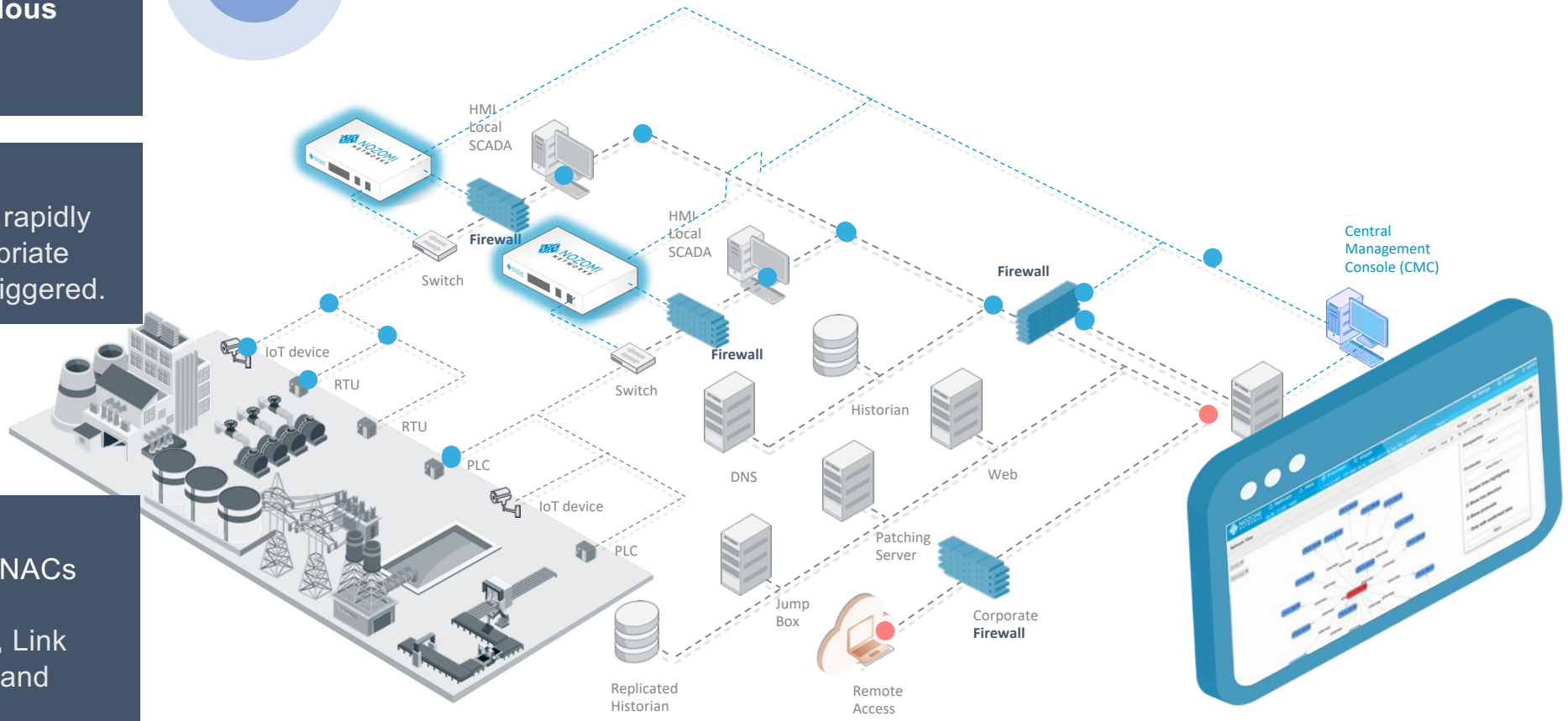
Best Threat and Anomaly Detection for OT/IoT

1) Monitor
Guardian detects **anomalous behavior** or **threats** and generates an alert.

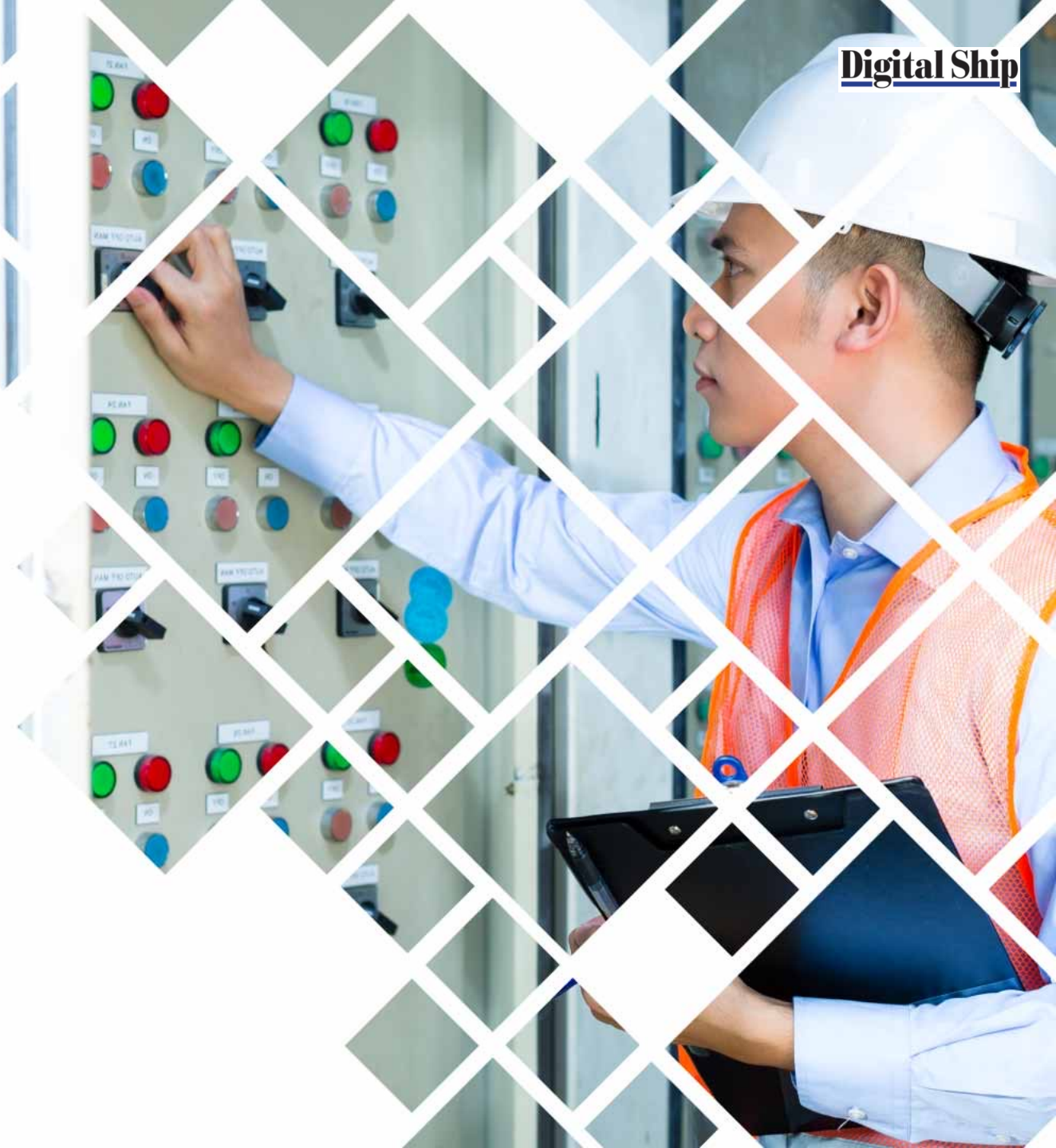
2) Detect
User-defined policies are rapidly examined, and the appropriate corresponding action is triggered.

3) Respond
Integration with firewalls, NACs and EDRs enables rapid response (Node Blocking, Link Blocking, or Kill Session) and mitigates the issue.

Dynamic Learning &
Adaptive Learning Accelerates Network Learning and Anomaly Detection



NOZOMI NETWORKS



Why NOZOMI NETWORKS

Nozomi Networks Strengths

Proven Scalability

Central Management & Analysis
Manage any number of sites & assets

Cloud Multi-tier Architecture
SaaS platform monitors any number of assets and locations from anywhere

Agentless Protection
Single Guardian sensor can monitor over 500K assets

Faster Deployment

Sensor Options to Fit Your Environment
Physical, virtual, cloud, edge, container sensors

Cloud Architecture
SaaS platform speeds onboarding, eliminates sizing issues

Industry's Largest Partner Ecosystem and Open API
Minimizes integration complexity

Always-On Monitoring

Continuous Monitoring of All Supported Protocols: OT, IoT and IT
No critical blind spots

Unmatched Detection & Visibility
Prevents operational disruptions

Audit-ready Default Configuration
Avoids findings due to misconfiguration

Full Stack Solution

No Reliance on Other Vendors
Avoids EOL impacts or waiting for patches

Rigorous QA Ensures Interoperability and Stability
Improves hardening, scalability, rollback, data analysis

Integrated Development
Extracts the best performance from hardware and software

Why Nozomi Networks

- ✓ Existing deployments on vessels and in harbors
- ✓ Designed to work off-line or over satellite com
- ✓ Centralized visibility of the entire fleet in the cloud
- ✓ Data analytics to help prioritize resources and budgets
- ✓ Alerts and incidents notification centrally in real time
- ✓ Specific maritime use cases
  - ✓ NMEA protocol support
  - ✓ Possibility to cover maritime specific situations with custom rules

THANK YOU!