TOTOTHEO
MARITIME

Cyber Security Solutions

Tototheo Maritime's Cyber Security Solution has received
a Certificate of Compliance by IACS Classifications Society RINA

Cyber Security Solutions

Complete and flexible cyber security solutions to protect your most valuable assets – your people, data, and vessels.

Cyber Security has always been an important factor when it comes to the maritime sector, but the rapid growth in cyber threats since the start of the digital age has brought a whole new dimension and urgency to ensure that ship owners, operators and crews can operate safely and securely.

As our industry is evolving through a fast-paced digital transformation, there is a great need to enhance efficiency while reducing costs. Our solutions leverage technology to improve every part of your business. However, this means there are new risks to manage: information security is multidimensional, and it applies to every operational level and procedure. With our solutions, you can implement robust measures to counter these risks. Our approach ensures the reliability of information under a secure environment that aligns with your business objectives.

The ISM Code, supported by the IMO Resolution MSC. 428(98), requires ship owners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system.

Expert Consultancy & Advisory

Gap Analysis

A gap analysis is the first step in identifying security improvement for your organization. Our experienced analysts assess your company's cybersecurity methods and present you with details of how they could be improved. This in turn serves to identify any vulnerabilities so they can be removed, thereby maximizing the effectiveness of your cybersecurity practices.

Risk Assesment

Through our Risk Assessment procedures, we identify the roles and responsibilities of users, key personnel, and management both ashore and onboard, as well as systems, assets, data, and capabilities that could pose risks to ship operations and safety. Additionally, our services implement technical and procedural measures to protect against cyber-attacks aboard the vessel. We will create response plans for cyber incidents to ensure continuity of operations.

Maritime Cyber Security Plan

Our expert team will deliver tailor made Information Security Policies and Procedures that ensure your organisation is compliant with existing applicable guidelines or regulations like BIMCO, IMO, TMSA3, RightShip, NIST, ISO 27001:2013.

Vulnerability Assesment

The objective of a Vulnerability Assessment is to scan, investigate, analyze and report on the level of risk associated with any security vulnerabilities discovered on public, internet facing devices and to provide your organization with appropriate mitigation strategies to address those discovered vulnerabilities.

Penetration Test

A vulnerability assessment is the process of identifying and quantifying vulnerabilities. Penetration Testing is designed to help you understand which flaws could be used in a real attack and to quantify the risk associated with each flaw. Combining penetration testing with vulnerability assessments gives a comprehensive picture of all security threats and their risk levels.
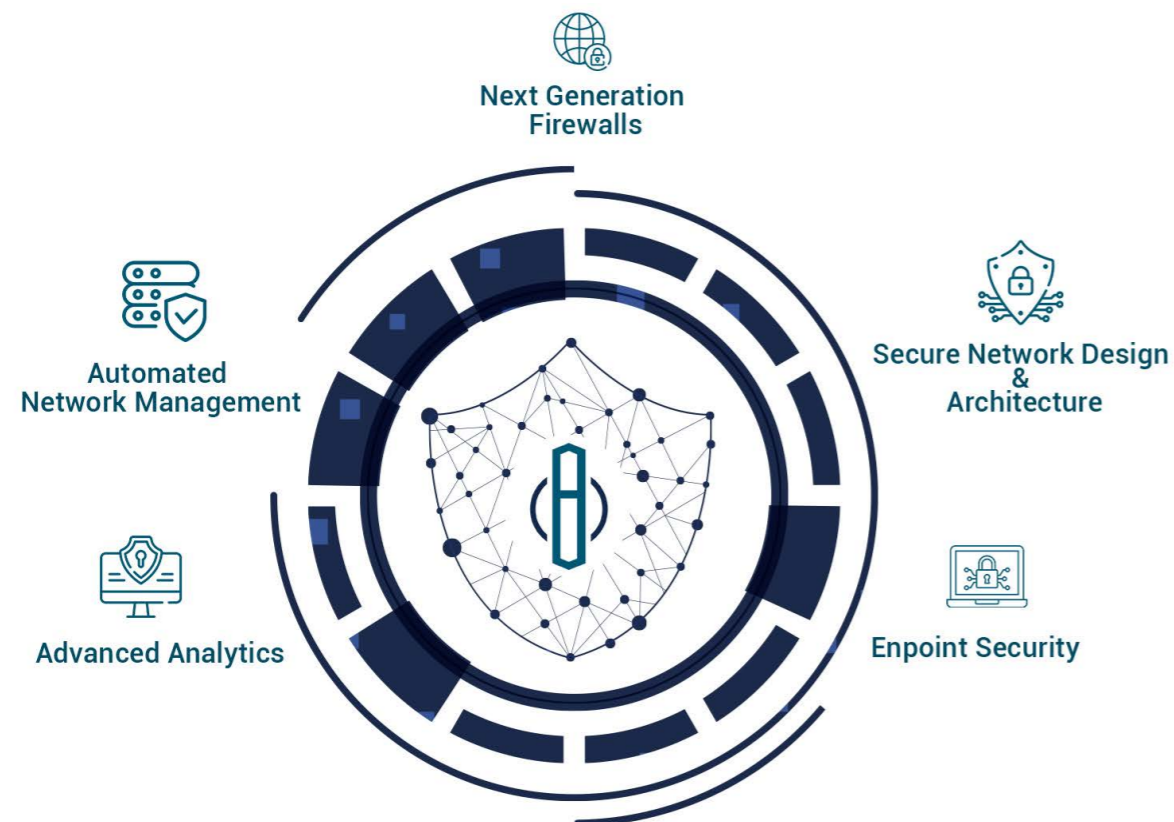
Sophisticated
Technology

Cyber Security Technology Services

Driven by the need to move faster at a global scale while reducing costs, companies are consciously or unconsciously, undergoing digital transformation. As data, devices and people move faster across multiple perimeters, security risks are increasing exponentially.

With our cyber security technology services at the core of your organization's architecture, you gain a uniformed, integrated, and secure end-to-end cyber security strategy.

A strategy that is easy to deploy, maintain, and continuously evolve — in full security compliance — for a successful digital transformation and business continuity.

Next Generation Firewalls

Automated Network Management

Advanced Analytics

Secure Network Design & Architecture

Enpoint Security

Next Generation Firewall & Unified Threat Management (UTM)

We deliver industry-leading network security at any scale with full visibility and threat protection.

- Ultra-fast security, end to end
- Consistent real-time defense
- Excellent user experience with security processing units
- Operational efficiency and automated workflows

Along with the UTM security services, our next generation firewall covers the BIMCO guidelines as well as the IMO requirements for limitation and control of network ports, protocols and services.

• Application control: allow, deny or restrict access to applications or categories of applications.

• Intrusion prevention system: detect, block and protect against latest network intrusions.

• Antivirus: protect your systems against viruses, spyware on an application layer.

• URL Filtering: protection by blocking access to malicious, hacked or inappropriate websites.

• Sandboxing: execute malicious files in an isolated environment in order to analyze and report regarding a potential threat before infecting any operational systems.

• SSL inspection: gain visibility into encrypted traffic and prevent encrypted malware reaching your network.

• Prevention of unknown sophisticated threats is achieved using the above combination of technologies.

Empower your operations with the industry's most agile technology required to protect the entire hybrid IT infrastructure.

Sophisticated
Technology

A cybersecurity mesh platform for advanced threats

Empowering our customers with the security intelligence needed to identify and block advanced threats. With a rich open ecosystem of applications that protects devices, data, and applications from cyberthreats at every layer of network traffic, our platform extends protection across every asset on your network—from the endpoint to the cloud.

Features & Benefits

High-performance threat protection
Industry's highest threat protection and SSL inspection performance to protect from malware attacks hiding in encrypted traffic.

Validated security effectiveness
Independently certified and continuous threat intelligence updates provide robust protection from known and unknown attacks.

Protect mission critical applications
Highly scalable segmentation and ultra-low latency to protect network segments.

Automated continuous risk assessment
Leverage automated workflow and auditing features to deal with scarce security staff and continuously maintain compliance posture.

Security Fabric Integration
Intelligently share threats across the entire digital attack surface to provide quick and automated protection.

Enterprise class security management
Deliver consistent security policy - Single pane-of-glass to manage security assets irrespective of location and form factor.

Simplifying your security operations with advanced analytics

The growing volume and sophistication of cyber threats and risks drives the need for analytics-powered security and log management that can provide greater visibility into network activity, resulting in more accurate threat detection, faster time to resolution, and prevention of breaches.

The solution accelerates the ability of security operation centers (SOC) and network operation centers (NOC) to detect, analyze, and mitigate cyber threats across networks and endpoints—while reducing the burden on security teams for more efficient threat management.

Features & Benefits

End-to-end visibility with event correlation and threat detection
Reduce detection time by leveraging Indicator of Compromise (IOC) service to quickly identify threat across your network.

Enterprise-grade high availability
Automatically backs up the database for up to four nodes in a cluster that can be geographically dispersed for disaster recovery. One of the secondary nodes can easily become a primary node.

Advanced compliance reporting
Provides hundreds of pre-built reports and templates which are regulation-specific to make proving compliance easy.

Security automation
Reduces complexity and cost leveraging automation enabled via REST API, scripts, connectors, and automation stiches.

Multi-tenancy and administrative domains (ADOMs)
Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective.

Increased security and a flexible platform for building advanced cyber defense solutions for increasingly complex environments.

Automated threat protection, complete visibility and control of your enterprise and endpoint devices.

Sophisticated
Technology

Endpoint Security

Our endpoint protection solution provides automated next-generation threat protection and enables security consolidation through transparent integration with an enterprise's existing security infrastructure and operations.

Its tight integration with our cyber security mesh platform enables policy-based automation to contain threats and control outbreaks.

Features & Benefits

Unified endpoint features including compliance, protection, and secure access into a single, modular lightweight client.

End-to-end threat visibility and control by natively integrating endpoint into the Security Fabric architecture.

Advanced threat protection against exploits and advanced malware.

Integrated patch management and vulnerability shielding to harden all endpoints.

Simplified management and policy enforcement with Enterprise Management Server (EMS).

Automated Network Management

To adapt to the ever-evolving security landscape, a network security strategy that prioritizes network automation can help reduce one of the leading causes of cyber risk and downtime—human error and misconfigurations.

Our automated network management provides centralized management, best practices compliance, and workflow automation to provide better protection against breaches.

Features & Benefits

Centralized management
Provides a rich set of tools to centrally manage 100,000+ devices such as firewalls, switches, and access points from a single console.

Enterprise-grade high availability
Automatically backs up the database to up to five nodes in a cluster that can be geographically dispersed for disaster recovery.

Secure SD-WAN provisioning & monitoring
Provision and monitor Secure SD-WAN from one console across all branch offices or campuses Advanced compliance reporting.

Security automation
Reduces complexity and cost leveraging automation enabled via REST API, scripts, connectors, and automation stiches.

Multi-tenancy and administrative domains (ADOMs)
Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective.

Protect your network, secure your data and assure compliance.

Manage your network with enhanced security, increased ease of use and streamline your operations to reduce the risk of breaches.

TM Security Operations Centre

Sophisticated Technology

TM Security Operations Centre (TM SOC) is a holistic security management solution to manage complex and global threats, reduce business disruption, and mitigate cyber-security related risks.

It provides incident management, 24/7/365 security monitoring and business intelligence in real-time to improve performance, reduce risk and comply with regulations.

TM SOC enables you to focus uninterruptedly on your business' core activities while our security experts rapidly **detect, respond, and recover** from threats when necessary.

Vessel Threat Management Ashore

Managed Detection & Response (MDR)

Totoheo Maritime provides 24×7 real time Managed Detection and Response services for all critical shipboard information technology and operational technology systems. Our team ensures proper analysis of data from all submitted security events, ultimately providing our clients with the advantage to identify, prevent and respond to cyber threats.

Endpoint Detection & Response (EDR)

Endpoint detection and response (EDR) is a set of cybersecurity technologies designed to protect a business's endpoints (mainly its IT systems), detect and remove malware or other malicious activity on its network, or respond automatically to identified threats in order to remove them.

Vessel Threat Management On-board

Vessel Network Analysis

A centralized, self-contained network monitoring solution based on a virtual appliance can provide real time intelligence that enables threat detection and containment; it also provides the ability to log events, prioritize the most urgent alerts, and manage the flow of data across the enterprise.
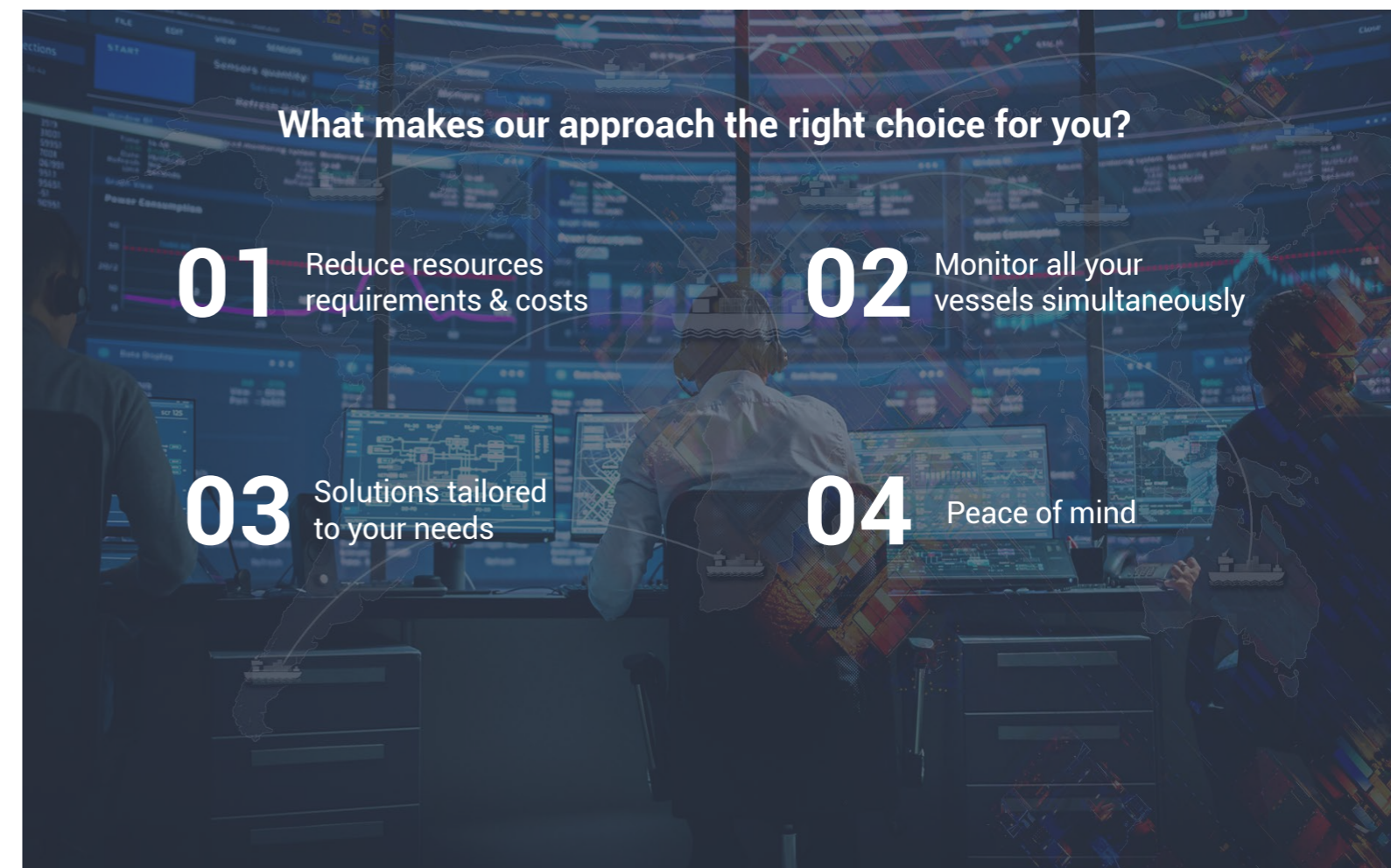
Endpoint Detection & Response (EDR)

A state-of-the-art Endpoint Detection and Response Solution for the IT systems on-board. With the most advanced technology, built-in cloud powered protection, industry-leading threat intelligence, and ease of deployment, our Endpoint Detection and Response solution gives you the most advanced protection.

Features & Benefits

- 24x7x365 Threat Monitoring
- Actionable Incidents Escalation
- Incident Case Management
- Active Incidents Containment (Endpoint Level)
- Threat Hunting
- Incident Response Services

- Threat Eradication Recommendations
- Log Retention
- Post Incident Investigation
- Threat Eradication & Recovery
- Root Cause Analysis
- Advisory Services

What makes our approach the right choice for you?

01 Reduce resources requirements & costs

02 Monitor all your vessels simultaneously

03 Solutions tailored to your needs

04 Peace of mind

Multidimensional Training

Maritime Cyber Security Awareness Course	Breach Detection and Incident Response	Custom Training Courses
• Maritime cyber security guidelines • Email security • Web security • Workstation security • Dangers related with USB drives • Malware infection • GDPR	• Threat detection analysis • Management of security incidents in information systems and networks • Ability to detect and deal with first level cyber-attacks	Each organisation is different in the way it manages its information security and relevant processes. We offer bespoke courses during which our experts will focus on the aspects you feel are important for your team.

We offer a wide range of cyber security courses that can be taught onsite at your company or online. There is no one-size-fits-all solution when it comes to cyber security training – each course is fully customizable, enabling you and your team to develop additional skills and be able to identify, prevent and respond to malicious threats.

We put a unique spin on your cyber security strategy.
Our focus is not just on risk mitigation and compliance, but also empowering your team to work safely and effectively.

Put your mind at ease with Tototheo Maritime.
We protect what matters the most.

www.tototheo.com