PORT-IT
SAFELY CONNECTED AT SEA

VANIR

ALL IN ONE MARITIME SECURITY SUITE

The maritime market is becoming an increasingly more lucrative target for cyber criminals. Many large ship owners, agents and even vessels have been hit with cyber security breaches, losing countless hours and potential funds in the recovery process.

Port-IT Vanir - the all-in-one Total Security Suite tailored to the maritime market.

Vanir integrates several Port-IT services and products into a single solution that is capable of tackling all cyber security threats our market faces today. Vanir is a service designed for VSAT or GX capable vessels.

With 24/7 active monitoring Port-IT is the first company in the maritime industry that raises the bar in cyber security. All of the components and features within Vanir can be configured and customized to your requirements by on shore staff using the Port-IT Web portal. All reports and logging can also be viewed in the portal.

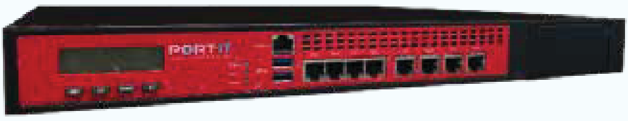
Vanir contains 5 major and 1 optional component. All components are completely shore manageable and contain smaller components that when combined create a well managed & near impenetrable infrastructure.

KEY COMPONENTS

- Complete network protection
- Advanced endpoint protection
- 24/7 monitoring, alerting & reporting
- Asset management
- Risk assessment
- Optional: Network detection & response (NDR)

WITH PROPER NETWORK SECURITY YOU CAN FORESEE THE FUTURE.

UTM SMARTBOX - A SINGLE SOLUTION



At its core Vanir leverages its extensive security set to protect the vessels network and its assets, but it also offers smartbox features such as routing, switching and more advanced networking features such as Dynamic DNS, link aggregation and secondary networks are also possible.

Features such as file synchronization, e-mail server and customer virtualization will allow you to get the most out of the Vanir platform. Leveraging its powerful hardware to lighten the load on your own hardware onboard.

Lightening the load of your internet connection is also important, the built-in quality of service and traffic management capabilities of the smartbox can ensure that vessel critical traffic always gets priority or even a dedicated amount of bandwidth.

VOIP and crew internet will allow you to stay in touch with the people on shore, all while being fully manageable, and monitorable from shore.

With a single solution, both the smart box and cyber security requirements of your vessel are covered.

A smartbox is a collective name for a device within a vessels network that can perform multiple tasks from a single device. Vanir offers these as dynamic modules that can easily be remotely enabled and disabled from a shoresid web portal, features such as:

- Software defined WAN (SD-WAN)
- Traffic management and QoS (quality of services)
- Integrated VOIP (Voice over IP) solution
- Customer virtualization
- Crew Internet
- File synchronization
- E-mail server (Orilla Mail)
- And many more..

NDR

Network Detection and Response (NDR) is a security solution used to detect and prevent malicious network activity, investigate and perform forensics to determine root cause, and then respond and mitigate. Therereby protecting organizations against cyber threats.

Implementing NDR will give organizations greater visibility into what is actually on the network as well as all activities. In turn, this will enable security teams to identify and stop suspicious network activity rapidly and minimize its impact on a daily business.

What does NDR do?

Port-IT NDR silently monitors the vessels network, watching for malicious events or suspicious traffic, even between devices only used internally, such as the VDR and a guest PC. Once this kind of traffic is detected the solution will deploy forensics, mitigate the issue and instantly informs the Port-IT Security Operations Center (SOC) team.

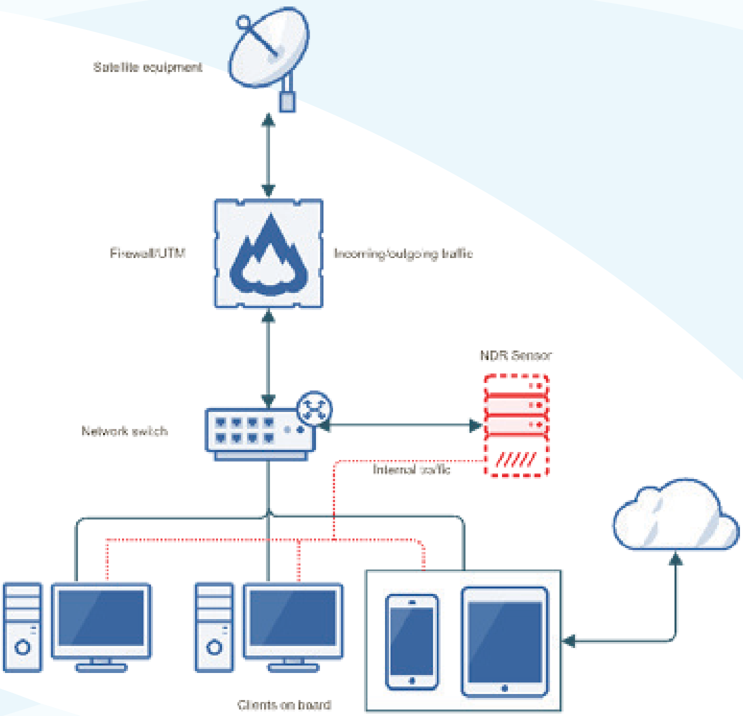
To detect malicious kinds of traffic it uses a combination of artificial intelligence, machine learning and userdefined policies, offering intelligent layers on which the configuration can be strengthened.

Port-IT NDR uses NTA, Network Traffic Analysis. NTA does not only monitor the network perimeter, but more importantly all traffic within the network for complete coverage. NDR detects threats across the entire network, including BYOD & IoT devices and even advanced unknown attacks that other solutions have missed.

NDR compliments the Vanir package to offer 100% visibility of all traffic in your network, and allows you to prepare your network for the cybersecurity challenges of today and tomorrow.

KEY FEATURES

- Top-of-the-line A.I. and machine learning;
- Integrates with existing firewall;
- Full visibility including BYOD & IoT;
- Can be integrated with Active Directory in order to identify users in your network;
- Identify events in multiple locations from one central point;
- Complimentary to existing security tools on board.



IMO 2021

As from 1 Januari 2021, IMO requires cyber risk management to be incorporated into ship safety management systems. The IMO recommendations can be summarised in 4 action steps:

Identify

Define personnel roles and responsibilities for cyber risk management, and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect

Implement risk control processes and measures, and contingency planning to protect against a cyber incident and ensure continuity of shipping operations.

Detect

Develop and implement processes and defences necessary to detect a cyber incident in a timely manner.

Respond

Develop and implement activities and plans to provide resilience and restore systems necessary for shipping operations or services halted due to a cyber incident.

Recover

Identify measures to back-up and restore cyber systems necessary for shipping operations that have been impacted by a cyber incident.

Recover
Identify
Protect
Detect
Respond

GDPR

Vanir is an excellent fleet wide implementation to enforce the new GDPR laws and regulations that have already been enforced since the 25th of May, 2018.

These laws are applicable to all EU citizens. Even if your vessel is not registered in an EU country you will still be subject to these laws. Vanir covers more than 16 of the 20 guidelines set up by the SANS top 20 Critical Security Controls which are recommended for enforcing GDPR. If your company is the victim of a data leak and you do not meet the requirements of these laws and regulations you can be held accountable. This can result in huge fines.

Vanir: pathway to compliance

All companies with seafaring vessels need to comply to the IMO2021 regulations. Onshore and offshore responsible persons need to know what is connected to the vessel's IT network. At the same time, measures should be taken in order to safeguard the IT network. Two components form the foundation on top of which security can be implemented: Uniformity and manageability. All of the components and features within Vanir will help cybersecure your vessel and at the same time prepares for IMO 2021 compliancy.

✉ **If you would like to learn more about Vanir or should you wish to receive a trial version or a free demo please contact us at sales@port-it.nl.**

Mackay
Marine Electronics & Satellite Communications
www.mackaymarine.com

Mackay Marine
+1 281 479 1515 marinesales@mackaymarine.com
Mackay Communications, Satellite Solutions
+1 919 850 3100 satserv@mackaycomm.com
Mackay Marine Canada
+1 902 469 8480 sales.canada@mackaymarine.com

PORT-IT
SAFELY CONNECTED AT SEA

Europe
Koperhoek 8 A/B
3162 LA Rhoon
The Netherlands

☎ **EMEA** +31 (0)10 260 00 41
APAC +65 31 58 16 17
✉ sales@port-it.nl
www.port-it.nl