VANIR ENDPOINT

ADVANCED ENDPOINT PROTECTION

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.

A conventional antivirus protects your machine from attacks that are launched from the files on the system itself but new forms of malware use the network to attack your system. A conventional antivirus does not protect you against these attacks like eternal blue and eternal romance used by viruses such as NotPetya. This leaves your critical systems vulnerable to attack.

Vanir Endpoint offers much more than a regular antivirus - with multiple layers of security it bolsters additional protection with much more security features. And on top of that it provides multiple asset management and monitoring options.

KEY COMPONENTS

- Advanced endpoint protection
- 24/7 logging and monitoring
- Asset management & network control
- Risk management
- Security reporting & visibility

ADVANCED ENDPOINT PROTECTION

Vanir Endpoint is powered by the Gartner-recognised ESET Endpoint Security – top rated against known and unknown threats of and awarded as one of the best solutions in the market. Combined with the advanced monitoring and reporting features, Vanir Endpoint gives users a greater sense of control and awareness over their environment.

Advanced endpoint security also includes:

Network attack prevention (NAP)
Network attack protection is an intelligent layer of security that is capable of detecting and halting network attacks such as Eternalblue, which was used in the widespread NotPetya attacks of 2017.

Botnet and ransomware protection
Botnet protection blocks the initial communication between the device and a malicious botnet.

Device, application and site blocking
Vanir Endpoint can block applications, connected devices such as USB flash drives and website from being accessed.

24/7 LOGGING AND MONITORING

Vanir Endpoint uses a powerful network scanning and monitoring module that will detect other devices on the local network that do or do not have Vanir Endpoint installed. Once installed detailed information such as installed programs, running processes and hardware will be collected and sent to the shoreside webportal.

RISK MANAGEMENT

Using the data collected via the asset management module a risk assessment can be performed to assist in IMO 2021 compliancy. The risk assessment will include all devices connected to the IT network and the information of the designated IT responsable person or entity.

SECURITY REPORTING & VISIBILITY

A full report can be created on the vessel, containing a record of all devices connected to the network, the hardware and the software that is installed. This report can be handed over to port state control and/or other authorities to show them the vessel has taken adequate steps to minimize the cyber security risks on board.

WEBPORTAL

All of the components and features within Vanir Endpoint can be configured and customized by onshore staff, using the Port-IT webportal. All logs and reports can also be viewed and downloaded here.

Cybersecurity is a necessity, not an accessory

IMO 2021 COMPLIANCY

Cyber preparedness is required to meet the IMO safety requirements. In order to comply, ships must be able to demonstrate what assets, personnel and procedures are in place on board and ashore to deal with cyber risk issues, what happens if systems are compromised and who has control. Compliance will depend on having the right risk management, infrastructure and procedures in place.

All of the components and features within Vanir Endpoint will help cybersecure your vessel and at the same time prepares

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