Forescout Enhances Cyber Resilience for the Maritime Industry

May 3, 2021

Forescout is first to support International Maritime Organization's (IMO) requirements by securing ship automation and control systems

SAN JOSE, Calif., May 03, 2021 (GLOBE NEWSWIRE) -- Forescout Technologies, Inc., the leader in Enterprise of Things security, today announced that the company's platform is the first commercial device visibility and control technology available to help maritime organizations meet specific Operational Technology (OT) security requirements prescribed by the United Nations' International Maritime Organization (IMO) for Maritime Cybersecurity.

As of January 1, 2021, maritime operators must comply with IMO's cyber risk guidelines . These measures address a wide range of strategic preparedness and technical controls, from evaluating the impact of cyber-attack scenarios, to implementing safeguards for bridge, cargo handling, propulsion, passenger-facing public Internet and other IT and OT systems. Ship owners and operators must ensure that cyber risks are appropriately addressed within IMO regulations and failure to comply with IMO 2021 may result in the denial of port access or even ship detentions.

"Modern ships are floating cities with navigation, propulsion, electric power generation, fuel dissemination and water treatment as well as other networked systems such as HVAC, video surveillance and automated safety controls," said Kevin O'Leary, chief product officer at Forescout. "With these expansive technologies, the damage a cyber incident can cause to critical systems can be far-reaching and difficult to contain due to poor visibility and control of all connected assets. Forescout has an established track record in maritime operations and now offers the power of complete operational technology (OT) network visibility and system integration with legacy and new bridge control systems."

Over the last three years, cyber-attacks on the maritime industry's OT systems have increased and the U.S. Coast Guard warned that "Legacy OT systems that were not designed to defend against current threats and activities, along with a failure to take necessary actions to protect newer systems and equipment, create opportunities for vulnerabilities and exploitation."

Maritime operators need to quickly collect and aggregate security and operational data from the entire control and automation systems of the port facilities and ships. This is essential to maintain safety, operational reliability and keep up with an evolving threat landscape.

Forescout provides maritime operators with complete device visibility and advanced threat detection for all marine control networks and monitoring applications. This expansive view of a ship's entire digital network increases the speed of detecting anomalies and threats while enhancing response and remediation across critical alarms to I/O and IP device networks. With Forescout eyeInspect, operators in port or at sea can mitigate or prevent operational issues before they lead to potentially dangerous incidents.

About Forescout
Forescout Technologies, Inc. actively defends the Enterprise of Things by identifying, segmenting and enforcing compliance of every connected thing. Fortune 1000 companies trust Forescout as it provides the most widely deployed, enterprise-class platform at scale across IT, IoT and OT managed and unmanaged devices. Forescout arms customers with more device intelligence than any other company in the world, allowing organizations across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Don't just see it. Secure it.

The Enterprise of Things – Secured. Learn more at www.forescout.com.

Media Relations Contact
Katie Beck
Forescout Technologies, Inc.
katie.beck@forescout.com

Source: Forescout Technologies, Inc.