

CASE STUDY

Norwegian Aquaculture Group Charts New Waters With Extended Security Infrastructure

First established in 1989 by private entrepreneur Inge Berg, Nordlaks has grown to become the largest family-owned aquaculture group in Norway with an annual production capacity in excess of 40,000 tonnes of premium Atlantic salmon and rainbow trout. In addition, the group processes a further 30,000 tonnes of fish from other producers in the region.

The current organization spans 12 municipalities in northern Nordland and southern Troms (regions in the north of Norway) and plays an important role in the regional economy, directly employing around 640 people but also creating around 1,200 ancillary jobs in supporting industries.

Critical to Nordlaks' success has been a continual process of technological innovation at every step in the production cycle, from roe to table. From the development of the world's largest spiral freezer (IQF) for whole fish in 2007, through the creative and profitable repurposing of fish-oil by-products in 2009, to the world's first hybrid LNG/battery-powered wellboat in 2021, Nordlaks has been helping to shape the future of healthy, environmentally sustainable aquaculture for the last three decades.

Most recently, and perhaps most ambitiously, following the granting of 21 new development permits in 2017, Nordlaks has launched the colossal Jostein Albert "Havfarm," a brand-new class of stationary sea farm able to bring sustainable fish-rearing to previously unusable sea and coastal areas.

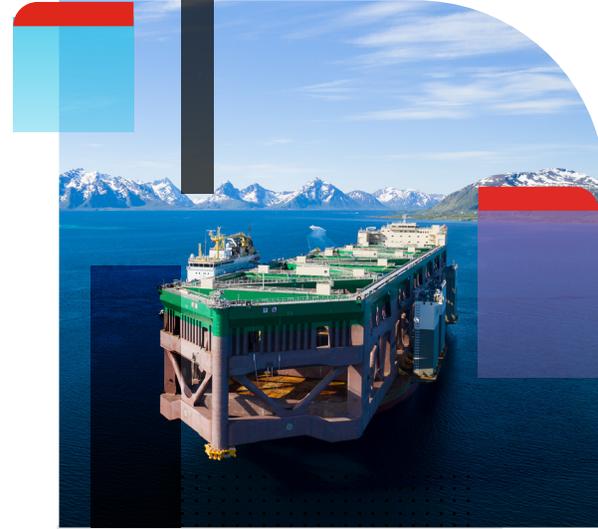
The Network and Security Challenges of Supporting Offshore Aquaculture

To support the healthy growth of valuable fish stocks, while minimizing their impact on the environment, every aspect of the farming process has to be closely controlled and monitored.

So, as part of a 10-figure NOK investment, and with a production capacity of 10,000 tonnes of valuable salmon, the 385m Jostein Albert had to be fitted with a comprehensive array of industrial monitoring and communications devices, connected not only to the onboard network operations center (NOC) but also to the rest of Nordlaks' land-based organization and data centers.

Furthermore, these systems, and the networking devices that interconnect them, had to be able to operate in the harsh conditions of the Norwegian Sea, with its subzero temperatures and frequent buffeting from rough seas and high winds.

"It's a very exacting environment and a business that demands zero downtime," explained Kurt-Erik Karlsen, senior architect for Nordlaks. "So high-availability and centralized management for broad visibility and rapid response are essential requirements for any new deployment."



"It's a very exacting environment and a business that demands zero downtime. So high-availability and centralized management for broad visibility and rapid response are essential requirements for any new systems."

– Kurt-Erik Karlsen, Senior Architect, Nordlaks

Details

Customer: Nordlaks

Industry: Aquaculture

Location: Norway

Business Impact

- Increased production capacity
- Secured remote monitoring of end-to-end farming process
- Reduced risk of downtime from security incidents or equipment failure

A Single Cybersecurity Platform for Protection, Monitoring, and Control

As a long-standing customer of Fortinet, Nordlaks had already seen the benefits of a cybersecurity platform, using the Fortinet Security Fabric to provide broad, integrated, and automated security to establish and maintain common policies across their existing land and sea-based operations. So, when it came time to choose network infrastructure components for the new flagship sea farm, Fortinet was the only logical choice.

With a portfolio that includes all of the high-performance, high-resilience, ruggedized products necessary for the project, Fortinet's position as preferred vendor was reaffirmed. Working closely with Fortinet's technical teams, the network was up and running by the summer of 2020.

The installation included FortiGate next-generation firewalls (NGFWs) for the connection to the rest of their existing infrastructure, FortiSwitch Rugged switches with Power over Ethernet (PoE) for interconnection between onboard industrial devices and cameras, and a network of FortiAP wireless access points spanning the vessel with wireless controllers to optimize traffic and further increase resilience.

With its purpose-built security processors, the FortiGate firewall has the power needed to identify thousands of applications inside network traffic and apply deep inspection and granular policy enforcement. This ensures that all of the traffic from Nordlaks' monitoring and control systems, together with all their business productivity applications, such as the cloud-based Microsoft 365 suite, are easily processed, optimized, inspected, and protected against potential threats without introducing latency into the network.

Fortinet FortiSwitch Rugged switches are engineered to deliver all the performance and security of a standard FortiSwitch, but in hostile environments where extreme swings in temperature might otherwise lead to component failures.

In addition, FortiSwitch's PoE capability simplified the installation of cameras, sensors, and FortiAP wireless access points on the vessel, with power and data delivered over the same network cable. This also helped to reduce the cost of installation as well as ongoing maintenance overhead.

The demanding environment of their innovative sea farm also required advanced wireless capabilities. To meet these requirements, Nordlaks chose the FortiWLC, a dedicated wireless controller that not only delivers high mobility across the farm but also superior reliability in a complex environment. By optimizing end device distribution and channel utilization in both single- and multi-channel deployments, the FortiWLC maximizes efficiency to make the most of the available wireless spectrum.

With every network security component linked through their integration with the FortiGate platform and its FortiOS operating system, the Fortinet Security Fabric is able to provide Nordlaks with consistent configuration and policy management and effortless, real-time communication across their entire security infrastructure. The FortiManager and FortiAnalyzer solutions then provide a centralized window and interface through which Nordlaks can monitor, analyze, and control that infrastructure to minimize the time needed for threat detection and mitigation and to reduce security risks that might arise from configuration errors or manual data compilation.

Solutions

- FortiGate
- FortiSwitch
- FortiAP
- FortiWLC
- FortiManager
- FortiAnalyzer

"That's the beauty of the Fortinet Security Fabric approach. Due to the integration across Fortinet's product range, new deployments are immediately covered under the same centrally defined security umbrella."

- Kurt-Erik Karlsen, Senior Architect, Nordlaks

“That’s the beauty of the Fortinet Security Fabric approach,” added Karlsen. “Due to the integration across their product range, new deployments are immediately covered under the same centrally defined security umbrella.”

Securely Enabling Innovation Through the Fortinet Security Fabric

By extending the existing network infrastructure out to the Jostein Albert sea farm at its anchorage just off the coast at Hadseløya, in the district of Hadsel in Vesterålen, Nordlaks can now safely monitor the health and growth of their fish in real time through an array of sensors and underwater cameras, whether onboard or remotely. This allows, for example, fine control of feeding systems to ensure that the right amount of food is released at precisely the right time to avoid waste and pollution of the local marine ecosystem.

For Karlsen and the team, because the new vessel is now fully covered by the Fortinet Security Fabric, they have full systems visibility, real-time monitoring, and detailed analysis of all new network traffic and devices from their network operations center back at headquarters.

Furthermore, due to the intelligent and adaptive nature of the Fortinet Security Fabric, as well as the breadth of functionality available through its component solutions, the team can rest assured that as further innovations drive new network requirements, their security infrastructure will be able to adapt accordingly.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.