

BW Offshore cuts the risk to its IT and OT environments with managed security services

Client profile

BW Offshore engineers innovative floating production solutions. They have a fleet of 15 Floating, Production, Storage and Offloading units (FPSOs) with potential and ambition to grow. By leveraging four decades of offshore operations and project execution, they create tailored energy solutions for evolving markets world-wide. BW Offshore's global presence, operational integrity and extensive experience leads the way in global floating production solutions for the oil and gas industry.

Which services?

- Managed Services
- Consulting Services
- Endpoint Prevention
- Cloud Access Security Broker
- Network Detection
- Threat Detection – Enhanced
- Device Management
- Digital Forensic and Incident Response Services

Which partners?

- Claroty



“

Working with NTT, we have a partner who can meet our requirements across both our IT and OT environments. This allows us to focus on enhancing the operational efficiency of our global fleet.

Enrico Piccini, Discipline Manager: Instrument & Telecom, BW Offshore

Summary

With operations across the world, BW Offshore understands the importance of securing both their IT and operational technology (OT) environments.

As OT and IT merged, systems that were siloed and protected are now open to cybersecurity threats that normally target IT systems. With operations across the world, BW Offshore viewed protecting their OT environment with the same priority as protecting their IT systems.

Together we created a cybersecurity strategy that ensured security across their IT and OT environments in line with their risk profile.

This allows them to deploy 24/7 threat monitoring of their OT environment where necessary, while incorporating key security processes and analysis across all their operations.

Business need

Securing the integrated IT and OT environment

Security is a critical component of BW Offshore's technology strategy. With vessels operating around the world, including West Africa, Brazil, the Gulf of Mexico, Asia and Europe, they needed to secure their IT and OT environments.

Each of these vessels contains an IT and OT environment, which, in the past, had been designed with an air gap to keep the systems isolated from each other.

The modern business environment, however, requires greater visibility into the operational environment, with information around production rates and equipment uptime required by executive teams.

'The amount of data that we'll be able to extract is only going to increase with digitalization. This will create real value for both the company and our clients, but before we can fully exploit this opportunity, we need a strong cybersecurity foundation in place,' says Enrico Piccini, Discipline Manager: Instrument & Telecom at BW Offshore.

To deliver this, BW Offshore created a security roadmap to ensure they're able to focus their efforts on the relevant areas of the business.

'Even though the IT and OT environments have different needs; visibility and monitoring are common requirements. In some cases this can be done as part of routine maintenance, but in others, such as our BW Catcher vessel in Aberdeen, we need 24/7 monitoring of the systems,' he says.

With the rapid evolution of the cybersecurity threat landscape, BW Offshore needed a partner to enable them to meet their specific needs.

Solution

Delivering 24/7 protection

Working with us, BW Offshore initially focused on the IT environment on their vessels and their global offices, to ensure protection against current and future cyberthreats.

At the same time, they analysed their OT environment, including security policies, standards, processes and controls, creating a full asset database and providing insight into potential risks, allowing them to apply resources and controls in the most effective way and adjust their strategy accordingly.

'These insights allowed us to incorporate security into our everyday operations, and deploy 24/7 monitoring of both the IT and OT environments,' says Fritz Ekløff, Head of IT and Systems at BW Offshore.

Using data from systems onboard the vessels our team of security analysts monitor the telemetry data and alert BW Offshore of any incidents. All data is routed through a central system at their Oslo head office, giving them full visibility of the data from their vessels.

With access to our global network of security operations centers, BW Offshore can leverage our comprehensive monitoring capabilities and advanced threat detection services. With our insights and next-generation analytics, they can take action to mitigate potential threats before they impact operations.

Outcomes

Creating a secure future

With the secure foundation in place, BW Offshore can explore the possibilities that greater visibility of their OT environment offers. Leveraging advanced threat detection and 24/7 monitoring they can deploy the most appropriate security solution for each of their vessels.

Secure IT environment

Leveraging our Security Operations Centers, BW Offshore are notified of any incidents in both their IT and OT environments and any potential impact this might have on production. They're also able to adapt the level of monitoring to match the risk profile of each vessel. 'Working with NTT we have a partner who can meet our requirements across both our IT and OT environments. This allows us to focus on enhancing operational efficiency of our global fleet,' says Piccini.

Opening up the data opportunity

With the potential to extract more data from their production environment BW Offshore can explore the potential that this offers, without incurring additional risk from connecting their OT and IT systems.

Working toward a sustainable future

BW Offshore is committed to environmentally conscious operations. By ensuring the security of their IT and OT systems, they're able to reduce the environmental risk that a cybersecurity incident might create. Leveraging our cybersecurity expertise provides them with skills across both IT and OT environments, minimizing the potential for miscommunication in the event of an incident.



The amount of data that we'll be able to extract is only going to increase with digitalization. This will create real value for both the company and our clients, but before we can fully exploit this opportunity, we need to have a strong cybersecurity foundation in place.

Enrico Piccini, Discipline Manager: Instrument & Telecom, BW Offshore