BARRIER

CASE STUDY

United Offshore Support selects Barrier Networks to secure its fleet of vessels against cyberattacks

Until recently, when most business leaders thought about cybercrime, their main concerns focused on monetary and data loss. They only viewed cyber as a digital threat. And while this still holds true, the real consequences of cyberattacks can often go far beyond digital today. In fact, cybercrime has shattered through its digital perimeters, and today we are seeing attacks impact society and the way people physically live their lives.

Take the 2021 attack on Colonial Pipeline; yes, the threat was targeted at the organisation's IT infrastructure, but the looting and fuel shortages directly impacted citizens. Or the more recent cyberattack on an Iranian steel manufacturer where the hacking collective Predatory Sparrow caused a physical fire. Again, the attack was digital, but the impact was very physical.

As a result of this increase in cyber/physical cyberattacks, many organisations are taking steps to improve the defences of not just their IT estate, but their connected Operational Technology (OT) as well. These organisations, which operate within industrial sectors, have come under heightened threat from cybercriminals because of modernisation within their environments, where OT is routinely being connected to the internet to cut costs and improve efficiencies. But if security is not rolled out in tandem, it also increases cyber risk.

This is one of the reasons why United Offshore Support (UOS) has recently appointed Barrier Networks to help improve the cybersecurity of its facilities.

UNITED OFFSHORE SUPPORT

Headquartered in Leer, Germany, UOS is a leading service provider to the global offshore industry. UOS has a fleet of 12 vessels which offer safe, high quality and cost-effective support services to the oil and gas industry, including rig moves and anchor handling.

Simon Lee, director of IT, started with the company in 2020 and recognised that as cybercriminals were turning up the heat on the energy sector, it was vital that UOS updated its cybersecurity program to protect against this increased threat.

"In the last few years, we have seen criminals set their sights on the energy and oil and gas industries, and as a key provider for offshore businesses, we recognised the need to ensure our systems and services were comprehensively protected. Our vessels operate very heavy machinery and regularly toe rigs around the world, so having one of our vessels compromised could have very dangerous outcomes not just for workers but also the environment,"

Simon Lee,
IT Director,
United Offshore Support

Lee recognised that as ransomware attacks were increasing across the globe, if infected with the threat, it could cause UOS downtime for offshore workers or close down systems entirely, which would be a catastrophic situation that he wanted to avoid at all costs. Furthermore, as UOS's OT was becoming more automated, he was also aware of the security threats this exposed the organisation to.

When it came to identifying a partner, Lee had worked with Barrier Networks at a previous organisation and knew it had the skills, expertise in IT and OT, and product portfolio to suit UOS's needs.

Barrier Networks is a UK-based managed security service provider. The company helps organisations build out cybersecurity programs, carry out risk assessments and penetration testing, train and educate employees of cyber threats, while also managing cybersecurity programs.

Barrier Networks also possesses unrivalled expertise in the field of OT cybersecurity, which was another one of the key attributes that attracted UOS. However, another key element was Barrier's suite of products. If UOS had gone to a cybersecurity product vendor, it would have needed to use the same product brands across all its infrastructure, regardless of whether it suited the organisation's specific needs. But, with Barrier being vendor agnostic, it uses the best OT and IT products on the market from various security companies, which provides increased security but also means products are selected based on a client's needs. Furthermore, since everything is embedded and managed by Barrier, it doesn't add to workloads or cause user friction; everything is managed efficiently under one umbrella.

Barrier has been working with UOS for over one year now, and the security is like night and day. Before Barrier came on board, the UOS cyber program was still in its infancy as the company had scaled quickly; however, all these issues have now been addressed, and the company now has a state-of-the-art security program that offers massive improvements to its cyber resilience. This has put the company light years ahead of where it was before working with Barrier.

The rollout was straight-forward and went exactly as planned, and Lee has been very happy with the management and customer support he receives from the Barrier team.

However, the biggest improvements have been around visibility, which is the foundation for any good IT and OT cybersecurity program. UOS can now see all of its assets, which means everything on the network is fully protected and visible to security teams; furthermore, everything can be seen through a single pane of glass, which makes security more accessible and easier to manage.

As for the future, UOS has more plans to continue working with Barrier as they scale the business and continue to automate OT processes.

So, would Lee recommend Barrier to his peers in the energy and oil and gas sectors?

"I'm a happy customer, and I'm a repeat customer, so that says it all really. I would never hesitate to recommend Barrier as they have the experience and expertise to keep their customers safe and secure, which, let's be honest, is getting more critical by the day in the cyber world," concluded Lee.