

# Dolphin Drilling Ltd



## A Safe Platform for Dolphin Drilling Ltd Sanctuary Provides Secure IT Environment for Remote Workforce

### The Company

Dolphin, is part of the drilling contracting business segment of Fred Olsen Energy ASA, and has undertaken world-wide offshore drilling operations since the company was established in 1965. Fred Olsen Energy provides exploration and production services to the offshore oil and gas industry, building on 150 years experience in shipping and more than 35 years in offshore drilling.

Dolphin manages and operates eight semi-submersible units and one deepwater drillship, which is permanently manned by a team of around 100 staff. Because of the nature of its operations, the company has to manage all the IT issues faced by a normal business, in remote locations, where it is difficult to get support staff out to the rigs in the event of downtime on the IT network.

### The Need

Dolphin Drilling Ltd, based in Aberdeen, recognised the need to counteract the growing threat posed by viruses, Trojans, worms and spyware to its computer network. Chris Message, ICT System Manager at Dolphin Drilling explains, "We have a number of specialised staff based out on the rigs, each vessel has between 10 and 30 PCs configured on a LAN, which is attached to our wide area network (WAN). We foresaw that with the outbreak of new worms

like Sasser, Blaster and other virulent malicious code, that we were at risk of losing parts of our WAN and facing severe downtime in the event of infection. Any downtime that disrupts our ability to communicate data to and from our head office in Aberdeen, or sub offices located in countries where we're operating, would be expensive to rectify in terms of lost productivity. Also, with the growing threat of spyware, we were keen to find a way of proactively removing the threat to our systems."

"Of course we are protected by the usual antivirus software and firewalls, but with the proliferation of new forms of worm, we predicted that this was only effective against the last known outbreak of malware. If a new worm or Trojan came on the scene, that could get around our antivirus software, we would have been vulnerable and we needed a way to prevent that. Also, with the limited number of staff based on the rigs, we simply could not afford the manpower to have staff running around installing fresh patches every time a new Windows vulnerability was announced."

Chris Message started looking for a solution that would supplement the existing perimeter security by protecting the PCs at the point of use. This would ensure that even if one of the machines got infected via a bad file being downloaded from the internet, or through a new virus causing a firewall breach, the malware would not be able to run on the machines and so the risk of downtime from infection would be eliminated.

### The solution

After looking at various types of security software on the market,

Chris Message decided to run a pilot of SecureWave's Sanctuary. This employs a "white list" approach, whereby only known and authorised software applications are able to run on each PC. Everything else is blocked from running. Sanctuary sits in the kernel of the operating system and actually checks the binary code of all software before allowing it to run. So even if a file looks like an authorised application, if there is a discrepancy in the binary code, it will be prevented from running on the machine.

The result is that Sanctuary creates a secure computing environment, where even if an employee inadvertently infects the machine through internet use, or through opening a bad file attachment, the malware will be prevented from running, so no downtime will be caused. In addition, malicious code used for stealing data will be prevented from activating on the machine, so no information will be leaked out while the machine is connected to the web.

### Comparative Study

Chris started off the pilot by installing Sanctuary on 12 machines in January 2003. As part of a phased roll out to compare and contrast the efficacy of the solution, some computers at Dolphin continued to be operated without the Sanctuary application having been installed. This paved the way for a revealing comparative study between those machines protected with SecureWave's Sanctuary and those protected only by antivirus and firewall security.

### The Benefits

Chris Message of Dolphin Drilling Ltd. described the success of the

implementation:

“After a year of running the pilot, we found that all the machines that were protected with Sanctuary were completely free of all known malware, but all those that we had not protected with Sanctuary had been severely infected with viruses, spyware and malware, despite the fact that the entire network was protected with antivirus software and firewalls. Sanctuary provides a secure environment for our staff to carry on working using the applications they need to do their jobs, without worrying about the latest spyware, Trojans or viruses disrupting their work or

compromising data security. Put simply, Sanctuary allows you to get on with the job, without compromising your network security”.

## Conclusion

The experience of Dolphin Drilling demonstrates the effectiveness of SecureWave's Sanctuary at preventing any malware, even the most malicious viruses, spyware and worms from compromising the integrity of a system, whether this is through information leakage or destabilisation of the platform. As Chris Message concludes, “When you're busy doing

what you're paid to do, Sanctuary relieves you of the need to become a security expert and allows you to get on with the job in hand, rather than being ruled by the latest security alerts and spending valuable time updating AV patches and firewalls in a knee jerk reaction. Also, because it only allows known, authorised and trusted applications to run, you don't have to be heavy handed with your staff security policy. Sanctuary ensures that enforcement is built in.”



**SecureWave**  
Safeguarding Tomorrow

[www.securewave.com](http://www.securewave.com)  
[info@securewave.com](mailto:info@securewave.com)

### North America

13755 Sunrise Valley Drive  
Suite 203  
Herndon, VA 20171  
United States of America  
+1 (703) 713 - 3960 Phone  
+1 (703) 793 - 7007 Fax

### United Kingdom

Midsummer Court  
314 Midsummer Boulevard  
Milton Keynes MK9 2UB  
United Kingdom  
+44 (0) 1908 357 897 Phone  
+44 (0) 1908 357 600 Fax

### Continental Europe and Rest of World

Atrium Business Park  
23, rue du Puits Romain  
L-8070 Bertrange  
Luxembourg  
+352 265 364-11 Phone  
+352 265 364-12 Fax

© 2007 SecureWave SA. SecureWave and Sanctuary are registered trademarks of SecureWave SA. All third party trademarks are the property of their respective owners.