CASE STUDY

Securing Onshore-Offshore Data Exchange for Mud Mixing Automation

Business Challenge

As part of an ongoing mud mixing automation initiative, our customer identified a critical requirement: secure and reliable communication between the onshore production facility and offshore operations. This connectivity enables the seamless exchange of operational plans, performance reports, and real-time updates that drive decision-making and efficiency. Because these data flows are highly sensitive and business-critical, involving proprietary information and operational parameters, any compromise could lead to safety or reputational consequences. To mitigate risk, the solution had to include robust cybersecurity measures ensuring confidentiality, integrity, and availability of all transmitted data. This was not just a technical enhancement, it was essential to safeguarding operational continuity and supporting the automation project's strategic goals.

HMH Solution

HMH provided a comprehensive security solution to facilitate the secure management and transfer of mud-mix system information.

The delivery consisted of:

- Deployment of a secure virtual environment
- Complete network design documentation
- Multi-level Intrusion Prevention System (IPS) and antimalware solutions, including application whitelisting, system lockdown, and USB port locking
- Verification compliance through DNV and customer internal requirements
- Solutions for license management, including antivirus/antimalware, IPS software updates, and backup licenses, with options for renewal and upgrades through HMH SecureOPS services

Overview

Objective

Enable secure and reliable communication between onshore and offshore operations for a mud mixing automation initiative.

Challenges

Protect highly sensitive, business-critical data flows while meeting compliance requirements and integrating with third-party networks.

Solution

Deployed a secure virtual environment with IPS, antimalware, and whitelisting, resulting in a verified, on-schedule installation that now enables protected onshore-offshore information exchange.

Securing Onshore–Offshore Data Exchange for Mud Mixing Automation

CASE STUDY

Site Scope

- Installation of required hardware and the Hyper-V virtual environment.
- Physical installation of the IPS into designated network cabinet.
- Coordination with the customer team for necessary power, connections, and work permissions.
- Software installation, including domain services, backup solutions, and database setup.
- Deployment of antivirus, whitelisting, and security software on all client systems.
- Execution of maintenance windows for seamless network integration, connecting the IPS securely between the Layer 3 Firewall and the third-party network.
- After installation, all systems operated in a “learning mode” for at least 7 days to analyze traffic patterns and applications in use. Full system activation and protection were put in place after establishing clear traffic restrictions among the Customer, third-party vendors, and HMH.
- On-site installation was conducted as per schedule.

Engineering Scope

- Provision and setup of a virtual environment running multiple secure virtual servers.
- Advanced IPS deployment.
- Establishing antimalware protection with application whitelisting, system lockdown, and USB port lockdown.
- Creation of a secure network design, including backup strategies.
- Preparation of logical network diagrams, zone and conduit documentation, and detailed risk and vulnerability analysis.
- Mark-up on customer drawings to illustrate solution integration.

Result

The solution was deployed, configured, and delivered on time. Installation at the site proceeded according to plan, resulting in a robust, secure, and verified infrastructure for automated mud process management and secure information exchange between onshore and offshore stakeholders.