Secure Connectivity for Oil and Gas OT Networks

BlastWave's OT Cybersecurity solution has been proven to reduce the time, cost, and personnel required to secure connectivity for Oil and Gas OT networks. BlastWave's solutions protect and secure connectivity for all sites across the upstream, midstream, and downstream O&G lifecycle. Some of the reasons customers choose BlastWave are:

Meet aggressive remote site cost targets: The BlastShield solution's cost model is straightforward to configure and scale, and remote sites can be added for minimal hardware and software costs compared to traditional IT solutions. The price model is straightforward: How many devices, users, and sites do you want to secure? Only a flexible software-based solution like BlastWave can deliver at O&G price targets for OT cybersecurity in sites with few devices.

Simplified Remote installation: The administrator can configure the BlastShield appliance remotely without sending IT personnel. Someone at the remote site simply plugs the appliance into the network, snaps a picture of its label, and sends it to the administrator. The administrator can then have the system join the BlastShield mesh network and apply all active policies.

Scale with Ease: BlastWave was able to go from 5k devices and 2k users to 18k devices and 5k users in less than 30 days at a large O&G customer, demonstrating both the scalability and ease of scaling up the solution across many remote sites.

Hard to Hack: Multiple customers have subjected BlastShield to extensive penetration testing, and none have been able to come close to hacking the system. This includes when insider compromises were simulated and lateral movement was attempted. BlastShield's ability to block reconaissance and credentials theft (since the system is passwordless), two of the attack vectors turbocharged by GenAI, ensure that the initial compromises that lead to breaches and hacks are prevented.

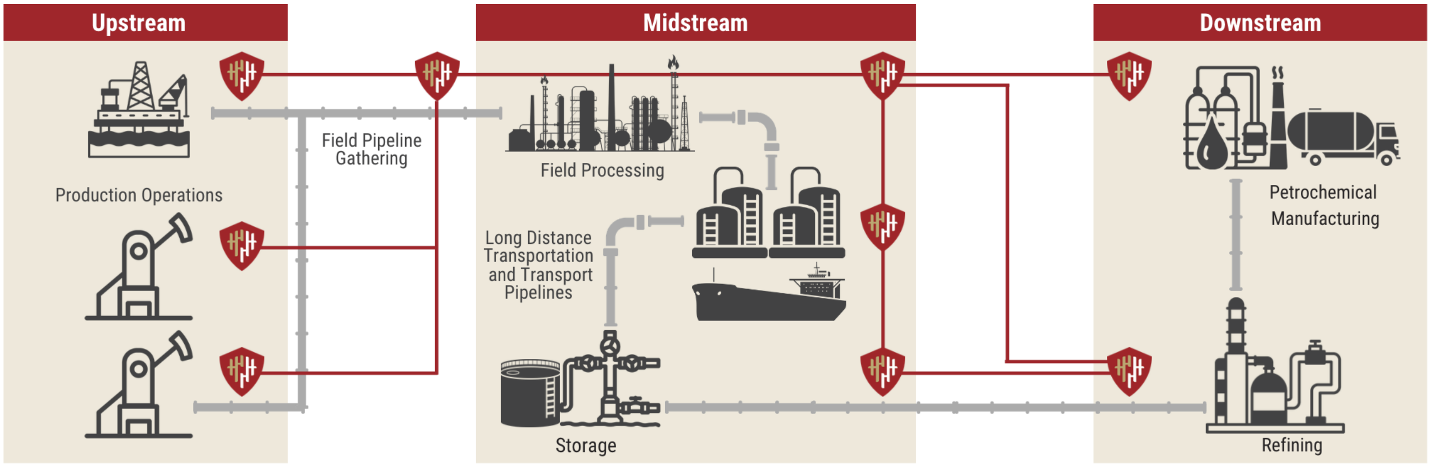
BlastShield Solution

Protect the Perimeter: Deploy in the OT DMZ and cloak the OT network from AI-powered reconnaissance and CVE exploitation of legacy OT devices.

Secure All Access: Connect remote sites and users with an encrypted software-defined network based on passwordless authentication and least privilege access.

Segment the Network: Create software-defined security zones and conduits based on risk to mitigate exploits and lateral movement in the OT network.

Figure 1 **BlastShield** in the Oil and Gas Ecosystem



BlastShield™: Zero Trust OT Protection for Oil and Gas Systems

Each oil and gas lifecycle segment has distinctly different cybersecurity requirements, which BlastWave uniquely solves to create an OT-specific security perimeter, adding to existing IT firewalls.

Upstream exploration and production require support for several remote devices at many sites. These devices require unattended operation with limited bandwidth and power. BlastShield's small form factor, one-touch remote configurability, and highly cost-effective pricing make it a perfect fit. The software can be deployed on commodity hardware and hits a sub-$1000 target price per wellhead, a critical upstream oil and gas price point.

Remote site connectivity should use secure communications and access to the site should be restricted to authorized personnel. BlastShield enables secure connectivity from any central site to remote sites through individual remote site deployments or as a centralized macro segmentation solution ideal for Upstream.

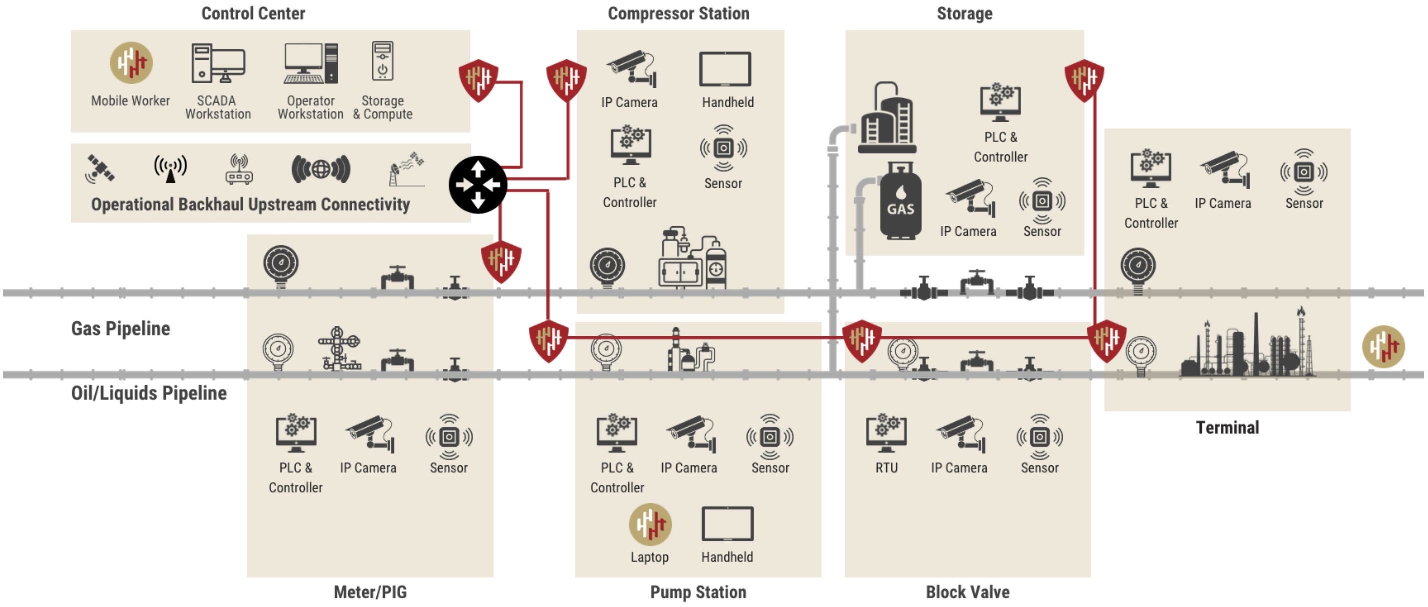
Midstream transportation and storage solutions require 24/7 uptime with strong remote management and monitoring capabilities. The devices must be small in form factor, ruggedized, and low power, as remote sites often have limited power infrastructure and bandwidth, a perfect fit for BlastShield.

By leveraging BlastShield's network cloaking, the Midstream remote sites are not discoverable from the rest of the OT network. This prevents reconnaissance from internal threats and protects them from hackers seeking to distribute ransomware into vulnerable legacy OT devices. BlastShield also secures access to remote pipeline sites and the more extensive storage and transportation hubs for midstream deployments.

Unlike other oil and gas lifecycle segments, the **Downstream refining, processing, marketing, distribution, and sale** of products require higher scalability and performance (including low latency) and stronger segmentation as maintenance contractors and temporary users are more involved in the logistics lifecycle.

BlastShield implements Zero Trust Protection to eliminate multiple classes of downstream risk. The solution combines the functionality of a cloaking firewall, Site-to-Site VPN, Remote Access VPN, Virtual Air Gap, and SD-LAN into a Zero Trust OT Perimeter Cybersecurity system perfect for OT networks.

Figure 1 **BlastShield** in Midstream Oil and Gas



v20250319

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499