BlastWave

SOLUTION BRIEF

AI-Resistant Cybersecurity Protection for Oil and Gas

The Operational Technology Challenge for Oil and Gas

The US has potentially millions of oil and gas wells and at least 144 refineries operating daily. That number is in the tens of millions of wells and hundreds of refineries worldwide. The output of the wells and refineries is then distributed and used by businesses and consumers.

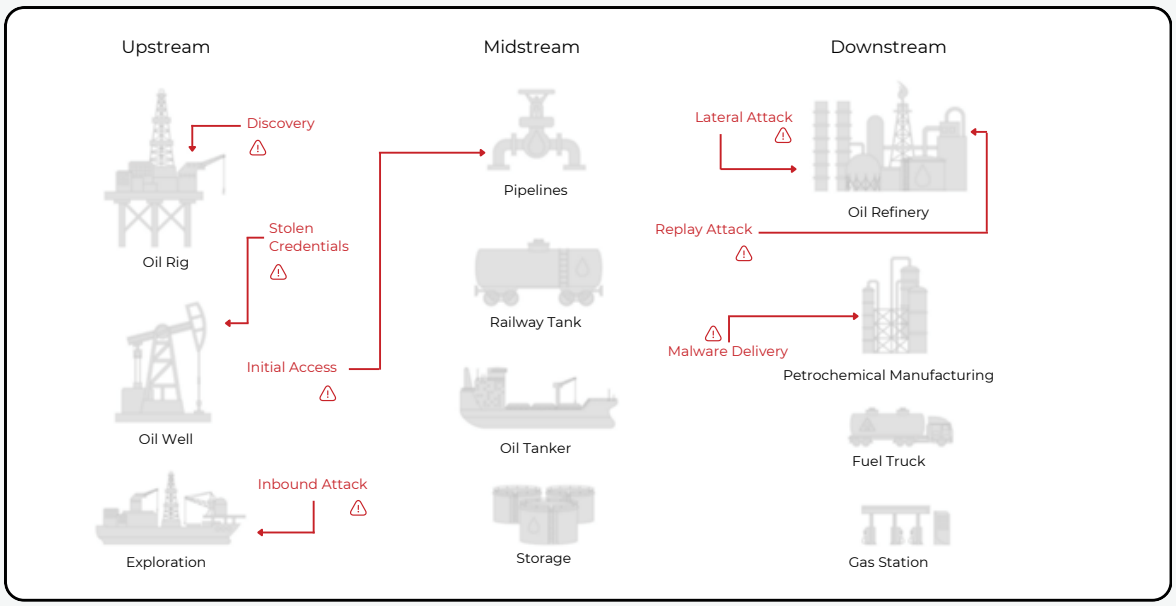
The oil and gas industry relies heavily on operational technology to manage a vast global energy assets and operations network. However, this reliance on technology makes the industry vulnerable to cybersecurity risks. The US Government Accountability Office has detailed significant cybersecurity risks to offshore oil and gas infrastructure, including those posed by threat actors, vulnerabilities, and potential impacts. The operational technology (OT) used to monitor and control physical equipment on sites has multiple known security flaws (CVEs). These flaws could allow attackers to remotely control critical safety functions, posing a severe threat to operational resilience. Outdated infrastructure, including old surveillance systems, may exacerbate these risks with fewer robust cybersecurity measures.

These risks spread across the entire oil and gas lifecycle, from Upstream exploration and production to midstream transportation, storage, and distribution and downstream distribution and sale.

BlastShield Advantages:

- Reconnaissance-Proof Software Defined Perimeter to prevent device discovery and vulnerability exposure with Network Cloaking
- Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- Delivers Least Privilege Access Policies and prevents Lateral Movement with Network Microsegmentation

Figure 1: Cyberthreats in Oil and Gas



BlastShield™: AI-Resistant OT Security For Oil and Gas systems

The oil and gas industry heavily relies on technology to control and manage critical operations such as drilling, refining, and distribution. A solution that protects their OT network and enables secure remote access is mandatory to keep the oil and gas industry operating smoothly. BlastShield is easily deployed as a simple migration without changing IT or OT network architecture. Installing and administering the solution takes an order of magnitude less time and effort than comparable solutions. The user experience is similar to Apple Pay, with simple biometric authentication granting access to only the devices the user needs.

BlastShield provides a PKI-authenticated secure gateway to the OT environment, where Industrial control systems, PLCs, IEDs, RTUs, turbine controllers, valves, and IoT devices remain in service for decades, long after vendors halt support. These systems often cannot be patched but require access to internal monitoring systems. BlastShield protects these systems from discovery by hackers by creating a virtual air gap with Network Cloaking, only allowing biometric-authenticated Secure Remote Access to the devices and leveraging Network Segmentation to create microsegmentation of different device types to prevent lateral movement within an existing flat Layer 2 network.

Network Cloaking

Network Cloaking ensures that critical yet outdated legacy infrastructure such as PLCs, DCSs, RTUs, SCADA, and HMIs become invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker. BlastShield ensures strong OT cybersecurity with the entire oil and gas supply chain. With Network Cloaking, AI-Enhanced reconnaissance tools cannot probe into the internal workings of a well or refinery because they have no path to reach the internal OT networks. Network cloaking proactively secures systems, making them invisible to potential attackers by blocking all internet access for legacy OT systems. It also creates a virtual air gap for OT systems that do not need access to the internet by only allowing them a hidden private address.

Secure Remote Access

BlastShield provides OT Secure Remote Access to critical upstream, midstream, and downstream systems, ensuring OT managers can monitor and manage them without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. A full mesh of P2P encrypted tunnels is created to secure traffic from remote users to the oil and gas facility and any agent-enabled systems, protecting against Man-in-the-middle attacks. Policy changes take effect in real-time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes.

Network Segmentation

BlastShield exceeds traditional segmentation by advancing the concept of microsegmentation as a superior security alternative. Unlike broad segmentation strategies, microsegmentation allows for incredibly detailed control, segmenting networks down to the level of individual devices, systems, protocols, or users. By isolating network segments, BlastShield effectively prevents the lateral movement of threats within the network, a critical defense mechanism against external and internal threats. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments. BlastShield's microsegmentation solution is innovative and future-ready for network security.

About BlastWave

BlastWave prevents AI-powered cyber attacks on critical infrastructure with a unique combination of Zero Trust Cybersecurity capabilities and delivers industrial-grade security with consumer-grade ease-of-use. Visit www.blastwave.com to learn more