

An industrial refinery scene at sunset. The sky is a mix of orange, yellow, and blue. Several tall, cylindrical distillation columns are visible, surrounded by a complex network of pipes, ladders, and structural steel. The foreground shows a perspective view of a walkway or platform with metal grating, leading towards the center of the refinery.

# **Zero Trust Protection** for the Oil and Gas Industry

Easy-to-Use Secure Connectivity

## The oil and gas industry is facing a growing number of cybersecurity threats, with AI-powered threats on the rise.

These threats can come from various sources, including nation-states, cybercriminals, and malicious insiders. A successful cyberattack can devastate an oil and gas company, leading to financial losses, reputational damage, and even physical harm. One of the biggest challenges facing the oil and gas industry is the increasing complexity of its IT and OT infrastructure. This infrastructure is often spread across a wide geographic area, making it difficult to connect and secure with expensive, complex cybersecurity solutions.

BlastWave's OT Zero Trust cybersecurity protection solution can help oil and gas customers with their most significant challenges:

**Reduced Costs:** Since BlastWave is more straightforward to purchase, install, and operate than other Zero Trust protection solutions, BlastWave takes 1/10th of the time, 1/2 the administrative lift in terms of management, and 1/4th the total cost of ownership.

**Eliminate Phishing Attacks:** BlastWave's Zero Trust approach helps improve an oil and gas company's overall security posture by reducing the risk of unauthorized access through credentials theft.

**Secure Connectivity with a Minimal Attack Surface:** BlastWave reduces the attack surface by limiting access to remote resources through network cloaking and targeted network segmentation.

**Improved compliance:** BlastWave helps oil and gas companies meet regulatory compliance requirements, especially with an IEC 62443 implementation of Zones and Conduits.

# CONTENTS

---

<b>Secure Infrastructure</b> for Oil and Gas	4
<b>Upstream</b> (Exploration and Production)	6
<b>Midstream</b> (Transportation and Storage)	8
<b>Downstream</b> (Refining and Distribution)	10



# Secure Infrastructure for Oil and Gas Networks

BlastWave's OT cybersecurity for oil and gas is like having a multi-layered defense system protecting every part of your operation. Upstream (exploration and production) has secured remote rigs and sensors from sabotage and data theft. Midstream (transportation and storage) has protected pipelines and control systems from disruption and leaks. Downstream (refining and distribution) has secured refineries and terminals to prevent explosions, spills, and fuel disruptions. It's all about keeping your people, assets, and the environment safe from cyber threats by securing connectivity and access.

**Oil and Gas OT Networks with BlastWave**  
BlastWave's OT Zero Trust Protection solution substantially benefits oil and gas companies, addressing critical security and operational challenges while driving cost efficiencies. By adopting a "never trust, always verify" approach, these organizations can:

## Secure Connectivity

Oil and gas operations often involve remote sites, third-party contractors, and mobile workforces. BlastWave provides secure connectivity by verifying user and device identity before granting access to resources. Passwordless MFA and contextual authentication ensure that only authorized individuals can access sensitive data and systems, regardless of location. This is especially important for securing remote access to SCADA systems and other critical infrastructure.

## Minimize the Attack Surface

OT networks in oil and gas are often complex and interconnected, making them vulnerable to lateral movement from compromised devices. BlastWave's micro-segmentation capabilities restrict communication to only authorized connections, limiting the impact of a breach. By enforcing least privilege access, organizations can minimize the potential for attackers to gain access to critical systems.

## Reduce Costs

BlastWave minimizes the need for costly, perimeter-focused security infrastructure. Traditional firewalls and VPNs often require significant hardware investments and ongoing maintenance.

Companies can optimize resource allocation and reduce capital expenditures by implementing software-defined access controls and micro-segmentation. Moreover, they can avoid incident response, remediation, and potential regulatory fines by preventing costly breaches.

## Improve Compliance

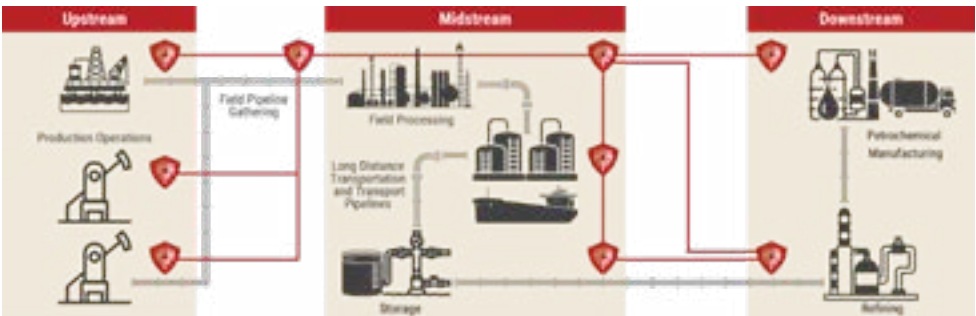
Oil and gas companies are subject to regulatory guidance like TSA and API standards. BlastWave facilitates compliance by providing granular visibility into network traffic and access patterns. Continuous monitoring and logging enable organizations to demonstrate adherence to regulatory requirements, simplifying audits and reducing the risk of penalties.



### BlastWave's Approach:

BlastWave implements a true Zero Trust architecture, assuming no user or device is inherently trustworthy. We verify every connection, enforce least privilege access, and continuously monitor network activity to detect and respond to threats in real-time. Our solution is designed to be easy to deploy and manage, minimizing disruption to existing operations.

By implementing BlastWave, manufacturers can strengthen their OT security posture, protect their critical assets, and ensure their facilities' continuous and secure operation in the face of evolving cyber threats.



An oil pumpjack is silhouetted against a dramatic sunset sky with orange and blue clouds. The pumpjack's long arm and counterweight are prominent. The scene is reflected in a body of water in the foreground.

# Upstream (Exploration)

## Securing Remote Drilling Sites

- Protecting remote drilling control systems, SCADA, and IoT devices from unauthorized access and manipulation.
- Enabling secure remote monitoring and control of drilling operations.

## Protecting Data Acquisition Systems

- Safeguarding seismic data, geological surveys, and other sensitive data from theft and tampering.
- Ensuring secure transmission of data from remote locations.

## Securing Offshore Platforms

- Protecting control systems and communication networks on offshore platforms from cyberattacks.
- Enabling secure remote maintenance and troubleshooting.

## Securing Pipeline Monitoring Systems

- Protecting the sensors and control systems used to monitor pipelines.

**Keep your people, assets, and the environment safe from cyber threats. Never trust; always verify.**

# and Production)

## BlastWave: Securely Connecting Upstream Onshore Exploration



## BlastWave: Securely Connecting Upstream Onshore Production



# Midstream (Transportation and Storage)

## Protecting Pipeline Control Systems:

- Securing pipeline control systems from unauthorized access, preventing disruptions to flow and potential leaks.
- Enabling secure remote monitoring and control of pipeline operations.

## Protecting Compressor Stations

- Protecting the control systems used to operate compressor stations.

## Securing LNG Facilities

- Protecting the control systems used in LNG facilities.

## Securing Storage Facilities

- Protecting storage facilities from unauthorized access and manipulation, preventing theft and environmental damage.
- Ensuring secure remote monitoring of storage levels and conditions.

## BlastWave: Securely Connecting Midstream Oil and Gas





# Downstream (Refining and Distribution)

## Securing Refinery Control Systems

- Protecting refinery control systems from unauthorized access, preventing disruptions to production, and potential safety hazards.
- Enabling secure remote monitoring and control of refinery operations.

## Protecting Terminal Automation Systems

- Securing terminal automation systems from unauthorized access, preventing theft and disruptions to distribution.
- Ensuring secure remote monitoring and management of terminal operations.

## Securing Distribution Networks

- Protecting distribution networks from unauthorized access, preventing disruptions to fuel supply, and potential safety hazards.

## Protecting fuel loading and unloading systems

- Third-Party Vendor Access:
- Providing secure access to third party vendors for maintenance and repairs.

## Protecting against AI powered reconnaissance

- Hiding critical network assets from AI-powered reconnaissance software.

## Phishing protection

- Using passwordless MFA to prevent phishing attacks against employees and contractors.

## Protecting legacy devices

- Using network cloaking to protect legacy devices that cannot be patched.

## Segmentation

- Using network segmentation to limit the blast radius of a cyber attack.

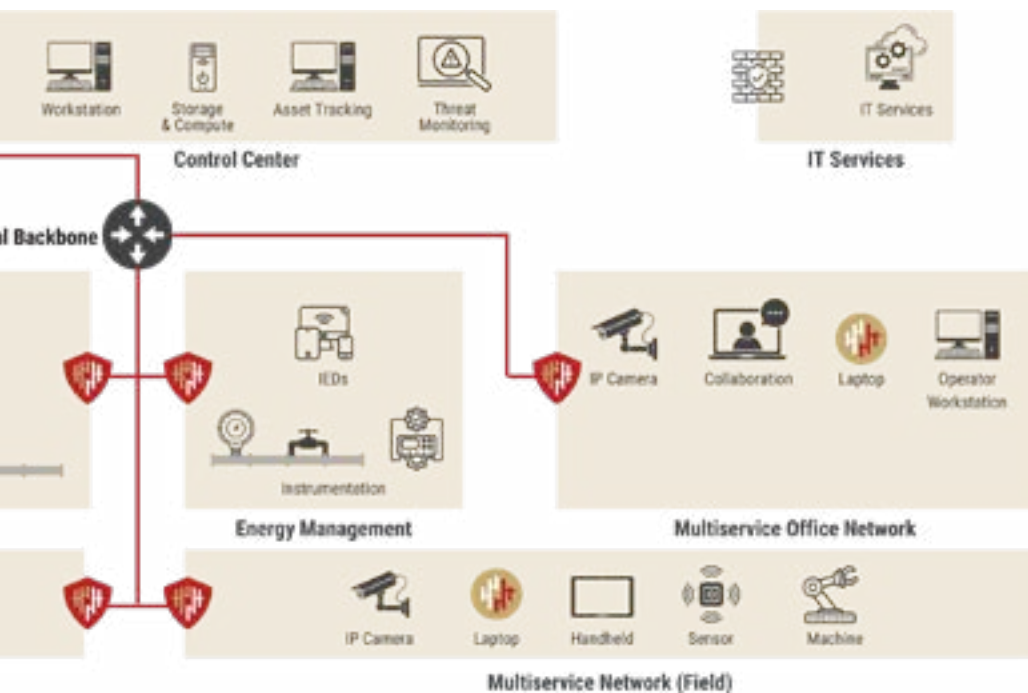
## Zero Trust

- Implementing a Zero Trust architecture to protect the entire network.

## BlastWave: Securely Connecting Downstream



## am Oil and Gas



## BlastWave's OT Protection Solution

---

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to  
[www.blastwave.com](http://www.blastwave.com)

v20260331

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at [www.blastwave.com](http://www.blastwave.com)



©2025 BlastWave Inc. | 1045 Hutchinson Ave., Palo Alto, CA 94301 USA | T: +1 650 206 8499