CUSTOMER STORY

How OPSWAT Enhances Intrusion Detection and Prevention in Critical Energy Infrastructure

Securing the Future of Global Energy with Advanced Operational Technology and Cyber-Physical Systems Protection

OPSWAT.
Customer Stories

Industry
Oil & Gas

Location
Global Operations with Multiple Sites in North America, Europe, and the Middle East

Size
Around 15,000+ Employees Globally

Products Used
MetaDefender OT Security™, MetaDefender Industrial Firewall™

About the Company

Our client, a leading global energy company, faced a critical challenge in securing its vast and geographically dispersed infrastructure. With operations spanning three continents and annual revenues exceeding $20 billion, they have established themselves as a key player in the global energy sector over the past four decades. Our client's operations are strategically organized across three business divisions: oil and gas, chemical and midstream and marketing. Their core oil and gas division stands at the forefront of energy resource development, from oil and gas exploration and production to storage, processing, transportation, distribution, and services. With over 50 production facilities in 12 countries and 15,000 kilometers of pipeline infrastructure, their diverse portfolio includes conventional oil and gas operations, condensate, natural gas liquids, and natural gas. Focused on reducing its carbon footprint, they also invest heavily in developing cutting-edge technologies in renewable energy for a low-carbon future.

What's the Story?

With sites spanning North America, Europe, and the Middle East, our client grappled with limited visibility into their OT (operational technology) assets and CPS (cyber-physical systems) security posture. The stakes were high: a successful cyberattack could disrupt operations, cause significant financial losses, and result in hefty fines. Given the interdependence of energy supply chains, disruptions could cascade through the value chain, affecting producers and consumers alike. OPSWAT deployed MetaDefender OT Security and MetaDefender Industrial Firewall into the client's OT & CPS infrastructure. This is the story.

A Wake-Up Call for Cybersecurity in Energy Sector

According to the S&P Global Platts Oil Security Sentinel™ research project, there have been 35 major cybersecurity incidents in the past five years targeting energy and commodities infrastructure.

The scale of this problem becomes clear when considering the digital footprint of a typical large-scale oil and gas company: hundreds of thousands of processors dedicated to reservoir simulation, petabytes of sensitive field data, and thousands of control systems distributed across multiple geographies, vendors, and partners. The vulnerability of this complex infrastructure was starkly illustrated by the Colonial Pipeline incident in 2021, triggering a state of emergency declaration by President Biden as gas stations across multiple states ran dry.

While Colonial Pipeline's experience served as a cautionary tale for the industry, it also catalyzed action. For our client, a leading global energy company, this moment prompted a comprehensive review of their security infrastructure. Yet, as the company's Chief Security Officer candidly admitted, their defenses were far from impenetrable.

> “Many of our facilities have legacy OT systems with limited security capabilities. Our existing tools were like puzzle pieces from different sets - they just didn't fit together, leaving us with significant gaps in our security posture.
>
> **Chief Security Officer**

OT Systems at Risk: Overcoming Visibility and Control Gaps

Lacking an effective incident containment and response strategy, the energy giant sought a solution that could provide granular, real-time insights into their sites while offering seamless deployment.

The company’s challenges were multifaceted:

1

Limited Visibility

Lack of comprehensive oversight of OT assets and CPS spread across various locations.

2

Process Control Gaps

Inability to monitor and control processes between critical OT devices, leading to potential security blind spots.

3

Fragmented Security

Disjointed security solutions failing to provide comprehensive protection and threat prevention.

4

Operational Inefficiencies

Lack of real-time insight into OT network activity and vulnerabilities, hindering operational efficiency.

5

Increased Cybersecurity Risks

Unmonitored or unpatched devices within the OT environment posing significant cybersecurity threats.

6

Regulatory Non-Compliance

Risk of fines and penalties due to non-adherence to a variety of regulatory requirements.

Embracing Integrated Solutions

As our energy client faced critical cybersecurity challenges threatening its global operations, its leadership recognized that piecemeal solutions were insufficient. After careful evaluation, the company made a strategic decision to partner with OPSWAT to implement MetaDefender OT Security and MetaDefender Industrial Firewall.

> With MetaDefender OT Security's comprehensive asset inventory and advanced threat detection capabilities, we can now swiftly identify anomalies and receive precise Exposure Scores to measure asset risk. Plus, its integration with MetaDefender Industrial Firewall lets us enforce strict security policies and block suspicious communications before they reach our PLCs and field devices.

Chief Security Officer

Enhanced Security Management

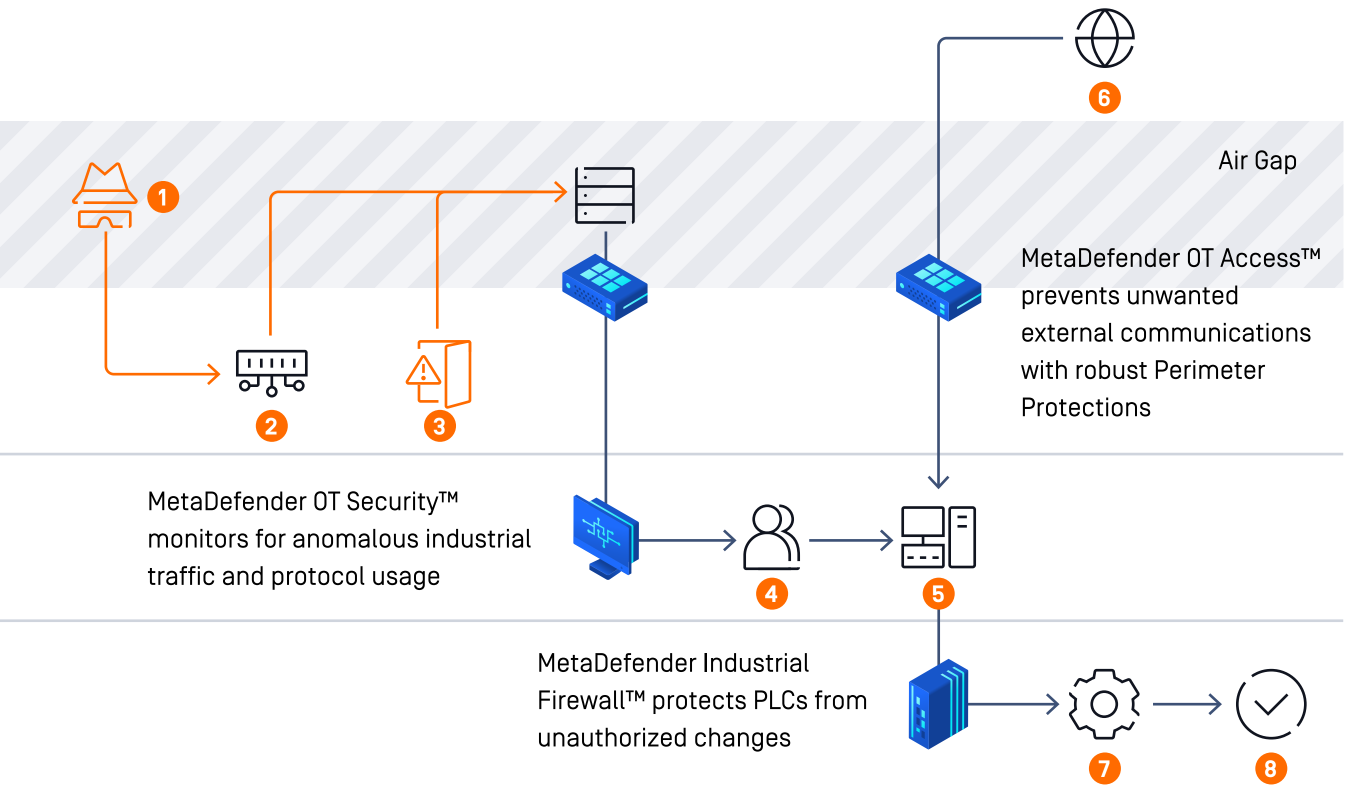
As the business expanded, keeping track of assets, network behavior, and data flow became increasingly challenging. MetaDefender OT Security provided comprehensive asset discovery, allowing the enterprise to gain real-time visibility into devices distributed across its refineries and production zones.

Now, security administrators could view detailed information on all OT assets, including vendor names, asset types and their statuses, firmware versions, latest vulnerabilities, misconfigurations, and more. With complete asset inventorying and network map, our solution enabled site managers to monitor network traffic and communications between these assets in real-time and identify anomalous behavior and potential vulnerabilities.

Comprehensive Threat Prevention

With their assets now visible, the next challenge was to protect them. For an energy company that managed a variety of complex operations, MetaDefender Industrial Firewall acted as the first line of defense through its native integration with MetaDefender OT Security. By dynamically segmenting the OT network, these ruggedized firewalls isolated unknown and suspicious devices from critical systems. Whether deployed at remote sites or production facilities, our firewalls were designed to withstand the harshest industrial environments, ensuring robust security across all facets of the client's operations.

Typical Attack Pattern in Energy Networks



MetaDefender OT Access™ prevents unwanted external communications with robust Perimeter Protections

MetaDefender OT Security™ monitors for anomalous industrial traffic and protocol usage

MetaDefender Industrial Firewall™ protects PLCs from unauthorized changes

1 Threat Actors
2 Vulnerable Modem
3 Webshell With Tunneling Accessed
4 Retrieve the SAM
5 Operations / Management Server
6 Establish Remote Connection
7 System Controllers
8 Process Disruption

Ease of Deployment

One of the key factors that influenced the company's decision to adopt OPSWAT's Critical OT and Cyber-Physical Systems protection solutions was their ease of use and quick deployment. Unlike other security solutions that struggle with OT complexities, MetaDefender offers a user-friendly experience and rapid implementation.

The AI Advantage: Adaptive Intelligence Against Cyberthreats

The integrated deployment of MetaDefender OT Security and MetaDefender Industrial Firewall helped the company proactively remediate detected issues, preventing potential threats from spreading across the network. A key feature was the AI-powered learning of normal traffic patterns, enabling both systems to distinguish between regular and suspicious activities. This adaptive intelligence minimized false positives while providing a more robust security posture. With this integrated platform, the company could gain complete visibility, stop evolving threats, and reduce the attack surface.

One Solution for Strict Compliance

Meeting compliance with industry regulations is not just a legal requirement—it's a matter of public trust and operational integrity.

The Chief Security Officer, who had long grappled with this challenge, found relief in MetaDefender's comprehensive approach: "Navigating the complex landscape of regulations is a daily task. A comprehensive asset inventory is fundamental to our compliance efforts."

The MetaDefender OT Solution was designed with a deep understanding of NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) compliance requirements, offering robust solutions for asset visibility, network monitoring, and threat detection. It even addressed the latest CIP-015-01 updates for INSM (internal Network Security Monitoring), ensuring that the company stayed ahead of regulatory curves.

Tangible Benefits

MetaDefender's integrated solution delivered a triple-impact advantage, enhancing business performance, operational efficiency, and security resilience. OPSWAT's defense-in-depth solutions ensured that energy infrastructure remains protected while optimizing operations and maintaining regulatory compliance. The operator can remain focused on energy generation and delivery, assured that its responders can perform their tasks without bouncing between multiple tools or gathering data from multiple sources.

MetaDefender's Integrated Security Solutions: Delivering Triple Impact

1

Business Benefits

- Scalable Asset Visibility and Inventorying Across Multiple Locations
- Reduced Cybersecurity Costs
- Improved Regulatory Compliance

2

Operational Benefits

- Enhanced Efficiency Through Improved OT Network Mapping
- Minimized Downtime with Smart Asset Management
- Protected Operations Through Network Segmentation and Zero-Trust Access Control

3

Security Benefits

- Proactive Vulnerability Detection and Remediation
- Rapid Threat Detection Through Automated Monitoring
- Advanced Threat Blocking Through Firewall Segmentation

A New Era of Visibility and Control

As cyberthreats continue to evolve, multi-layered solutions are needed to combat them. Our client's experience demonstrates that with the right defense-in-depth strategy, this challenge can be transformed into an opportunity for operational excellence and industry leadership. OPSWAT's MetaDefender integrates seamlessly with critical energy infrastructure to take more active defense measures without the hassle of complex, costly, and time-consuming implementation. By easily deploying MetaDefender OT Security and MetaDefender Industrial Firewall, our client was able to modernize and protect its network at scale, enabling faster troubleshooting and improved operations.

To see how OPSWAT's innovative solutions can keep your critical infrastructure safe, talk to an expert today.

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.