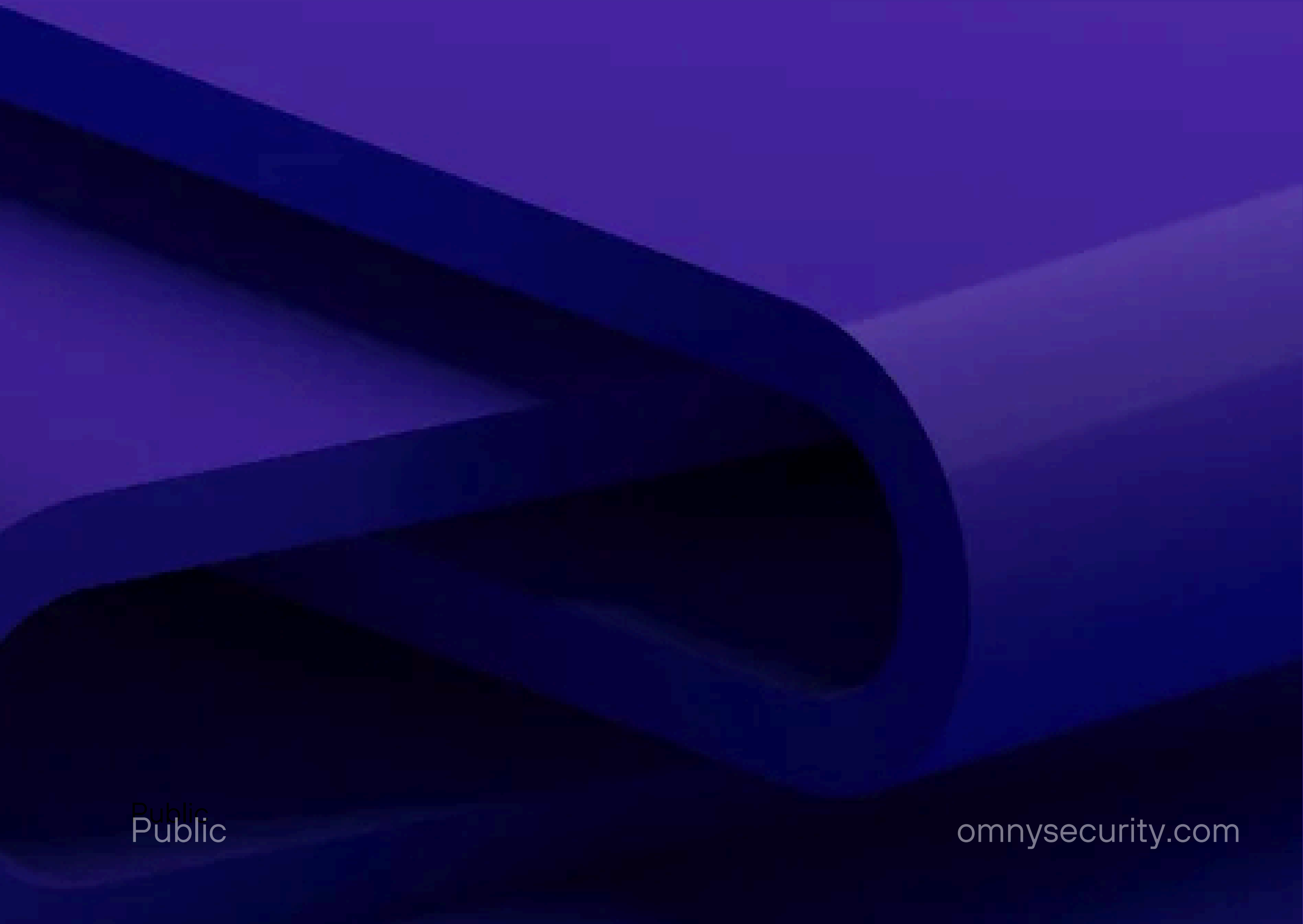
Version 1.0

Solution Brief

Omny for Oil & Gas

Securing production in complex, high-consequence oil & gas environments



Public

Public

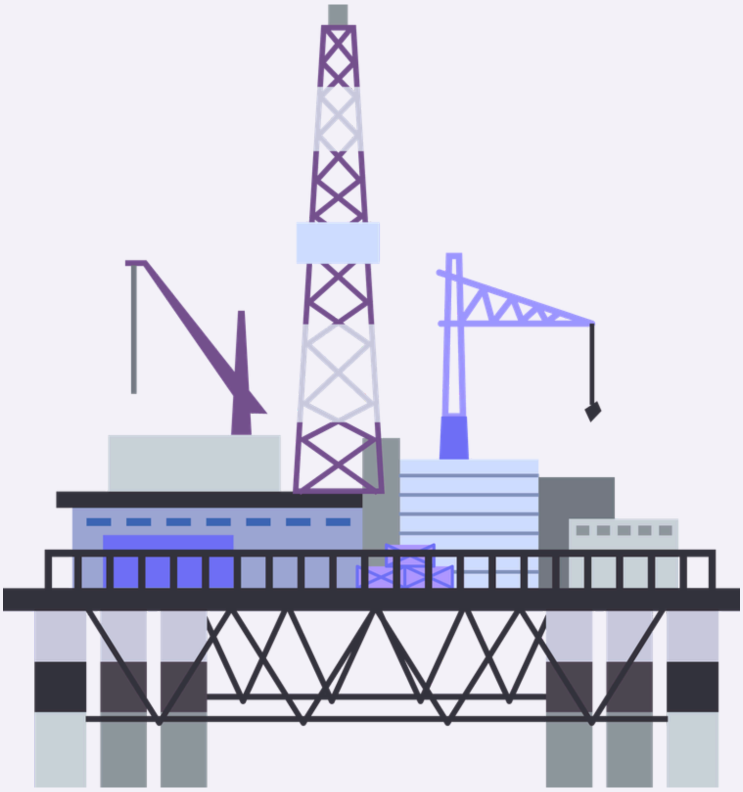
Table of Contents

Omny for Oil & Gas

Overview

Oil and gas operators run assets where a single misstep can halt production, damage equipment, or put people at risk. Offshore platforms, onshore facilities, and global supply chains depend on tightly connected IT and OT systems to keep operation stable and safe.

Digitalization and AI have made great strides in improving efficiency and enabling remote operations. At the same time, it has increased the interdependence between cyber systems and physical processes. Cyber incidents in oil & gas environments can disrupt production, trigger environmental consequences, expose the company to regulatory scrutiny, reputational damage, and in worst cases, put lives at risk.



Cybersecurity Challenges often faced by Oil & Gas Teams

For many oil and gas companies, one of the key challenges is to strengthen security without hindering production and profitability.

Omny helps oil and gas organizations manage this balance by providing a structured, risk-based view of assets, vulnerabilities, incidents, and security posture across IT and OT environments.

Top challenges oil and gas operations

1. Balancing security and production

Security investments must support, not stand in the way of, production. Asset managers and operational leaders continuously weigh risk against uptime and revenue. Demonstrating the operational value of security measures is often difficult, especially when its impact is preventive rather than visible or immediate.

2. Manual and resource-intensive vulnerability handling

Vulnerability handling is often time-consuming and document-driven. When a new common vulnerability and exposure (CVE) alert is received, teams must determine whether it affects their systems, whether it can be exploited, and whether it should be patched. This typically involves reviewing large volumes of documentation across extensive assets, communicating with vendors, and the communication of potential effects.

3. Fragmented visibility across IT and OT during incidents

Incident response requires close coordination between IT teams, OT experts, asset owners, and oftentimes vendors. These groups may not utilize the same terminology, systems, or data. Gaps in understanding can slow down investigation or mislead decision-making at precisely the moment when time is of the essence.

4. High-impact consequences of delayed response

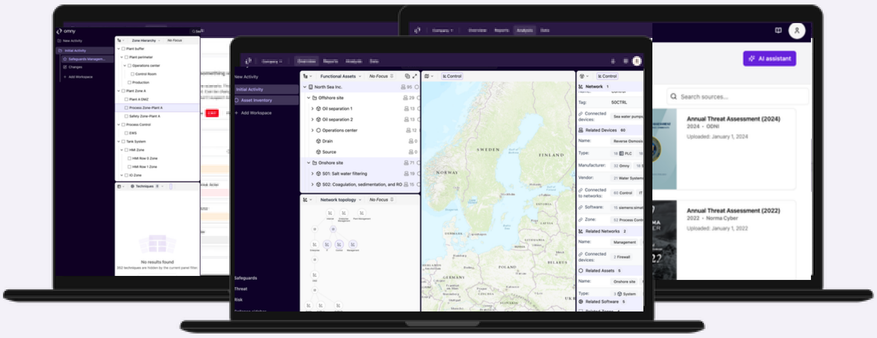
When incident response is unclear or delayed, companies may take drastic decisions such as shutting down entire systems to avoid escalation. This can result in production loss, environmental exposure, financial penalties, and safety risks. In offshore environments, escalation chains must function under pressure, and clarity around which processes are affected is critical.

5. Unstructured security posture and compliance insight

Security risk assessments, mitigation plans, and compliance documentation are often distributed across static documents. Some assessments may be outdated while still being used for audit purposes. Organizations lack a continuous, structured overview of what they are protecting, how it is protected, and whether current measures are still effective.

How Omny supports oil & gas organizations

Omny connects asset visibility, vulnerability insight, and operational context in one structured platform, supporting better decisions across vulnerability handling, incident response, and security posture management.



Asset visibility with clear ownership

Omny provides a structured overview of assets and devices and enables tagging of responsible owners. During both daily operations and incidents, teams can quickly identify affected systems and who is accountable. This reduces time spent searching for information and results in faster coordination.

Risk-based vulnerability prioritization

Instead of manually reviewing documentation for each new vulnerability, teams can assess CVEs in the context of their actual asset inventory and operational criticality. Omny supports structured evaluation of relevance and impact, enabling clearer prioritization and more effective communication of the remaining risk to decision-makers.

Contextualized incident response

Omny supports incident response by helping teams understand which processes are affected, how IT and OT environments intersect, and where responsible owners are located. It provides visibility into dependencies and backup locations, supporting more targeted containment and faster recovery. This helps reduce the likelihood of unnecessary shutdowns support business continuity.

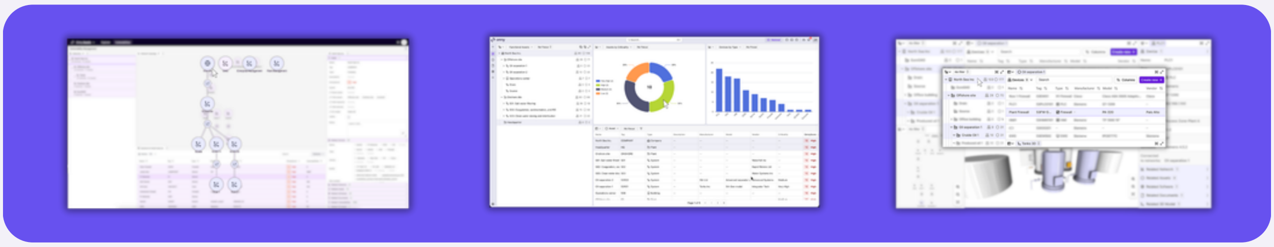
Structured, continuous security posture insight

Omny consolidates scattered documentation into a structured, risk-based view of security posture. Organizations gain clearer insight into how well their security measures work and where they remain vulnerable. This supports more informed prioritization and strengthens audit readiness without relying on static and often outdated reports.

Outcomes oil & gas organizations can expect

Oil and gas organizations using Omny can achieve:

- *Improved balance* between security and production through risk-based prioritization aligned with operational criticality
- *Faster and more coordinated incident response* across IT, OT, asset owners, and vendors
- *Reduced operational disruption* by enabling more targeted containment and clearer recovery planning
- *Stronger and more structured compliance posture* through continuous visibility into risk and mitigations
- More *efficient use of security resources* by reducing manual vulnerability assessment effort



Supporting security maturity complex environments

Omny supports oil and gas organizations at different stages of security maturity. For companies with fragmented documentation and limited asset visibility, Omny helps create structure and insight. For more mature organizations, it supports more efficient prioritization, clearer communication of risk, and stronger alignment between security and production.

In high-consequence environments, security must be operationally grounded. Omny helps oil and gas operators strengthen resilience while keeping production stable and people safe.

About Omny

Omny exists to protect industrial operations against cyber incidents. As industries rapidly digitize and the boundaries between IT and OT disappear, organizations must safeguard not only their digital systems but also the physical processes and assets that keep operations running. Our platform was designed to give visibility and context-rich insights to cybersecurity teams and operational stakeholders alike to give cross-functional understanding. Built on deep domain expertise and grounded in operational technology, Omny helps organizations secure critical infrastructure in an increasingly connected world.
Omny has an international vision with its headquarters in Oslo, Norway, and an additional office in Stavanger, Norway.

To learn more about our products and services, find us at omnysecurity.com or reach out to us at info@omnysecurity.com.

omny