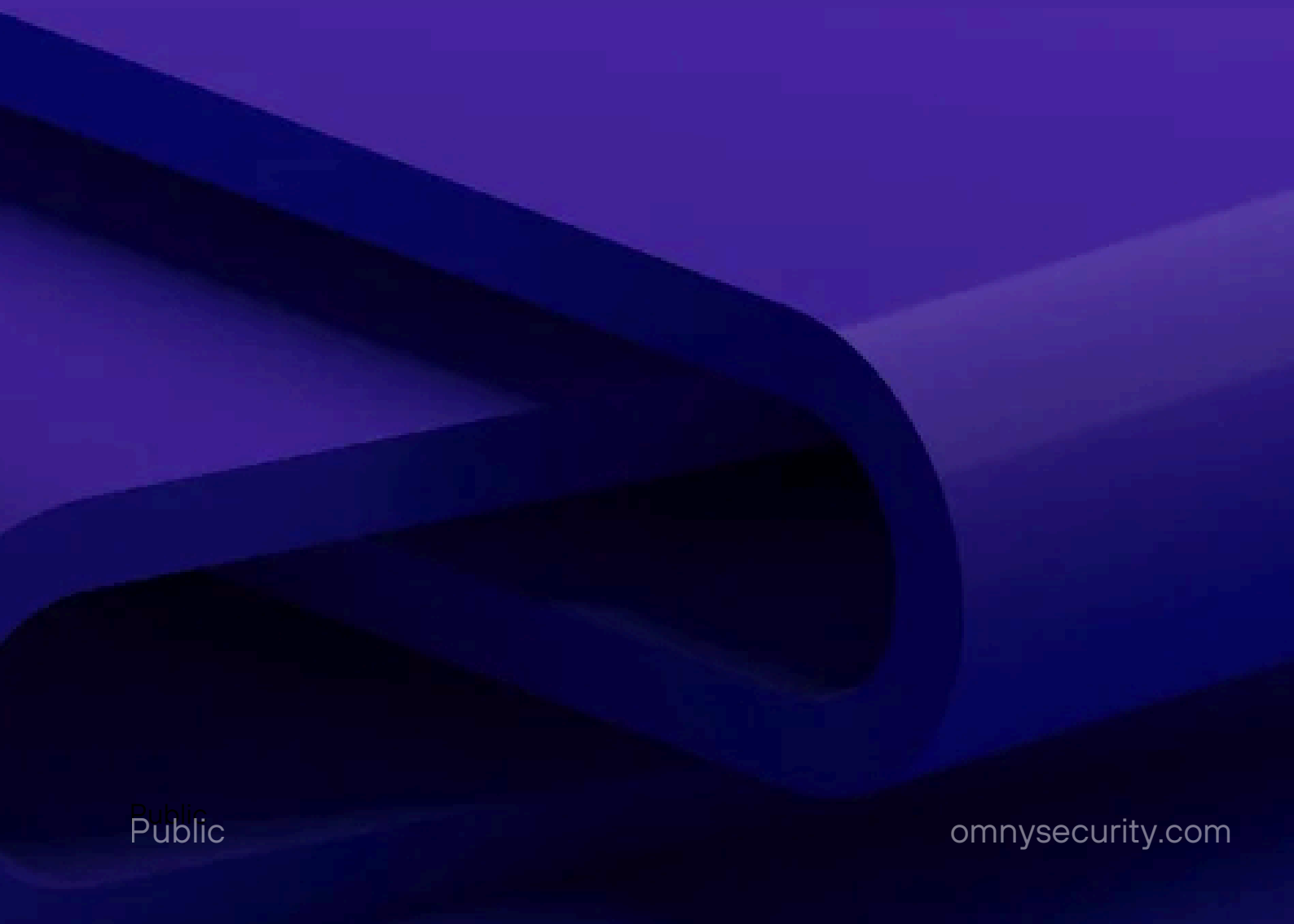
Version 1.0

Solution Brief

Omny for Power & Utilities

Secure operations in a cyber-physical world



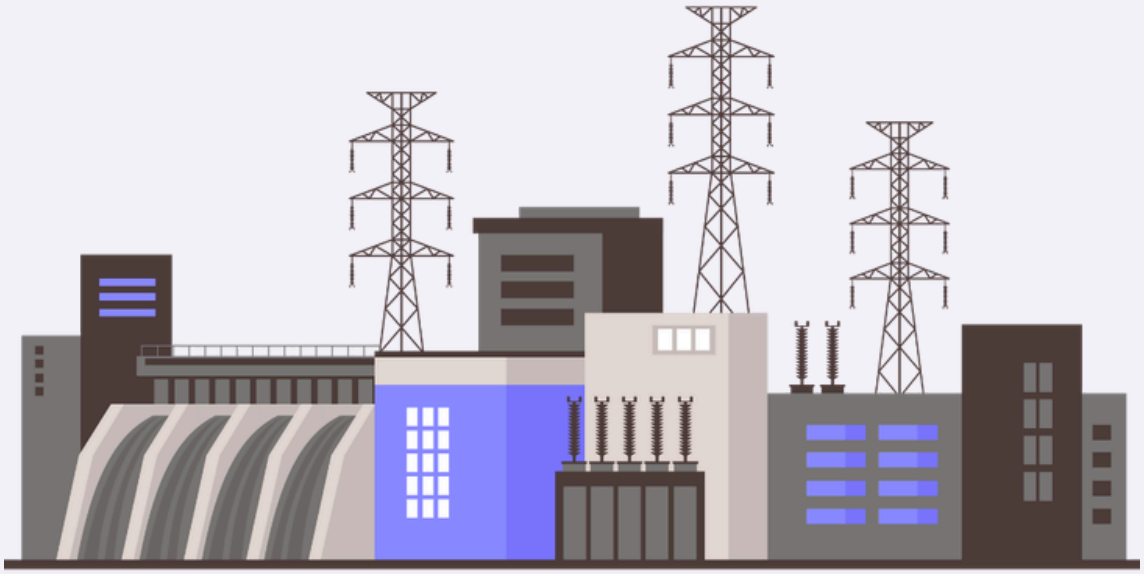
Public

Table of Contents

Overview

Power and utilities companies are on the road to modernization. Smart meters, digital substations, remote operations, and distributed energy resources are improving efficiency and resilience, but they have also led to a larger attack surface. Cyber incidents are no longer limited to IT systems, rather they can result in physical consequences such as outages and disruptions to create instability and potentially impact public health.

For many utilities, the challenge is maintaining operational reliability and meeting regulatory requirements while simultaneously managing cyber risk across highly complex, cyber-physical environments. Due to the great public impact an attack can have on one of these companies, it is oftentimes an appealing target for threat actors.



Cybersecurity Challenges often faced by Power & Utilities Teams

Omny understands the need for your organization to stay resilient against potential attacks, so we provide a unified, operationally grounded view of your full environment. We include IT systems, operational

Omny helps power and utilities organizations address this challenge by providing a unified, operationally grounded view of security risk across IT, OT, and physical assets. Unlike traditional methods to address operational problems, Omny's fresh approach gives security insights across all of these domains.

Top challenges power & utilities face

1. Rapidly expanding and changing asset landscapes

Digital substations, IEC 61850 environments, smart meters, sensors, and grid-edge devices are being deployed at scale. Many struggle to maintain an accurate, continuously updated picture of what assets exist, how they are connected, and how critical they are to operations.

2. Cyber risk with physical consequences

Incidents in digital systems increasingly affect physical operations, leading to shutdowns, voltage instability, or loss of service. Traditional IT-centric security tools lack the operational context needed to assess real-world impact.

3. OT-IT convergence without shared visibility

Integrated operations platforms and centralized control rooms bring IT and OT closer together, but security and operations teams often work from different data sets, tools, and priorities. This slows decision-making during incidents and increases risk.

4. Regulatory pressure and audit complexity

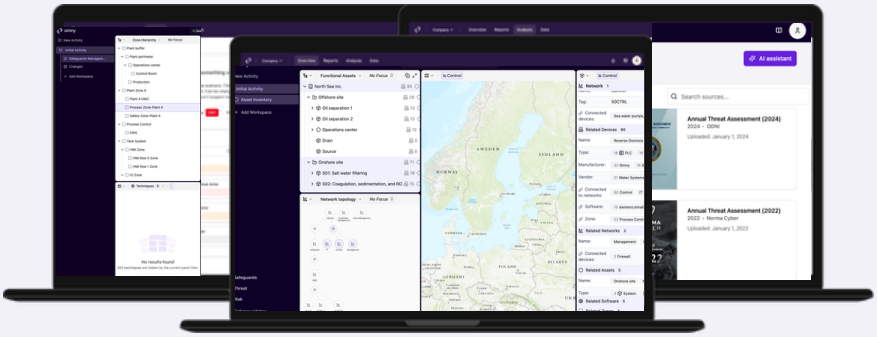
Frameworks such as Network and Information Systems Directive 2 (NIS2), Critical Entities Resilience (CER), national energy security regulations, and emerging EU legislation require utilities to document control of assets, risk, incidents, and supply chains. Manual reporting and fragmented data make compliance both time-consuming and fragile.

5. Limited specialist resources

NIS2 creates a unified framework for consistent cybersecurity practices across all EU member states, simplifying compliance for cross-border operations.

How Omny supports power & utilities organizations

Omny provides one integrated platform that connects technical security data with operational context, enabling utilities to prioritize what matters most when it comes to reliability, safety, and compliance.



Live asset visibility across IT, OT, and physical domains

Omny continuously maps assets across the Purdue model, from enterprise IT systems to substations, field devices, and physical infrastructure. This creates a shared, trusted view for security and operations teams.

Risk and threat insight grounded in operational reality

By combining asset criticality, vulnerabilities, threat intelligence, and operational dependencies, Omny helps teams understand not just where weaknesses exist, but which ones matter most to grid stability and service continuity.

Smarter vulnerability and patching decisions

Omny supports data-driven vulnerability handling by assessing common vulnerabilities and exposures (CVEs) in the context of operational impact, maintenance windows, and system criticality, which helps reduce unnecessary disruption while improving risk posture.

Contextualized SOC and incident response

Security alerts are enriched with operational context, enabling security operations centers (SOC) teams to assess potential physical consequences quickly and coordinate effectively with operations during incidents.

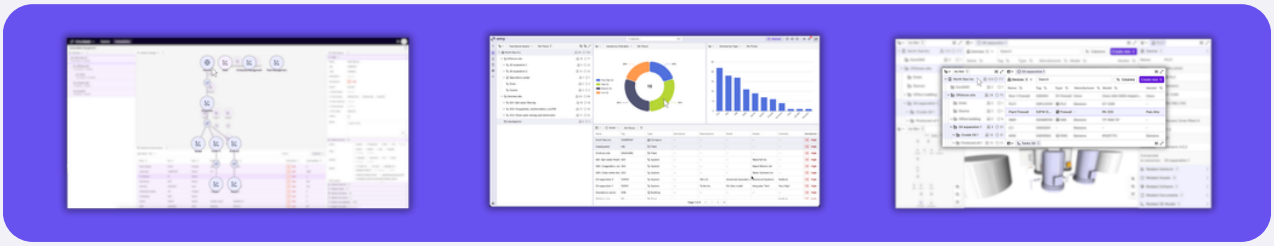
Simplified, continuous compliance

Omny provides live insight into security maturity and compliance status, supporting evidence-based reporting for regulations such as NIS2 and other critical infrastructure, without relying on manual data collection.

Benefits of Omny for Power & Utilities customers

Power and utilities organizations using Omny can achieve:

- **Improved operational resilience** through better prioritization of cyber risks that affect physical systems
- **Faster, more confident incident response** based on shared situational awareness between security and operations
- **Reduced downtime and operational disruption** by aligning security actions with operational constraints
- **Stronger regulatory posture** with continuous visibility into compliance and risk management
- **More efficient use of scarce OT security resources** through automation and contextual decision support



Designed for complex, regulated environments

Founded in Norway and developed in close collaboration with industrial and critical-infrastructure operations, Omny is built for environments where reliability, safety, and trust are non-negotiable.

Omny supports power and utilities organizations on their security maturity, helping them progress on their digital modernization journeys while keeping critical infrastructure up and running. Learn more about how Omny can support secure, resilient power and utility operations.

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.