SOLUTION BRIEF

Protecting Your Complex Energy and Utilities Environment with Armis

© Copyright Armis 2025

Introduction

The Energy and Utilities sector is responsible for providing some of our most basic human requirements, from powering homes, businesses, and critical infrastructure to supplying safe water. This sector encompasses energy generation, transmission, distribution, and other utility services, and relies heavily on Operational Technology (OT) to maintain the integrity and reliability of these essential systems. An interruption, even briefly, due to a security breach, can lead to potentially catastrophic consequences, including widespread power outages and potential loss of life.

Larger energy utilities face the reality of cooperative service agreements that share networks of IT and OT devices, which require constant monitoring and maintenance. The sheer volume of information and data produced in these environments that ensure a balanced service delivery without power spikes or brownouts must be automated - the use of manual spreadsheets just isn't realistic. Let's take renewable energy as an example, where energy outputs are not constant, and smart grid technology aligns with supply and demand, IoT sensors produce huge amounts of data critical to the operation of the grid.

Without some form of automation, vulnerability prioritization and remediation assignment, alert fatigue, or events being missed altogether is inevitable. Smaller utilities or electric cooperatives are being increasingly targeted by cyber terrorists and rogue factions which is increasing the need for a converged IT/OT security approach. These organizations tend to have one or two security employees overseeing IT, SCADA, SaaS, and email while simultaneously assisting other departments when called upon. With individuals so stretched and security initiatives largely under-resourced, buying back time to deal with vulnerabilities effectively is essential.

Unfortunately the "run to failure" method, where digital security in OT and CPS networks is used until it stops functioning effectively, despite the risk, can occur in heavy industries such as the energy sector. It's an approach that leads to unplanned downtime, aging infrastructure, compounding safety concerns, and legacy data buildup, all while leaving organizations vulnerable to cybersecurity threats and regulatory penalties. The grid itself has regular physical maintenance done. Trimming trees around wires, replacement of physical parts etc because as an industry, proactive maintenance is crucial. So the question must be asked, if we wouldn't dream of running the grid to failure, why from a digital security perspective would we take this risk?

© Copyright Armis 2025

The Energy and Utilities Landscape

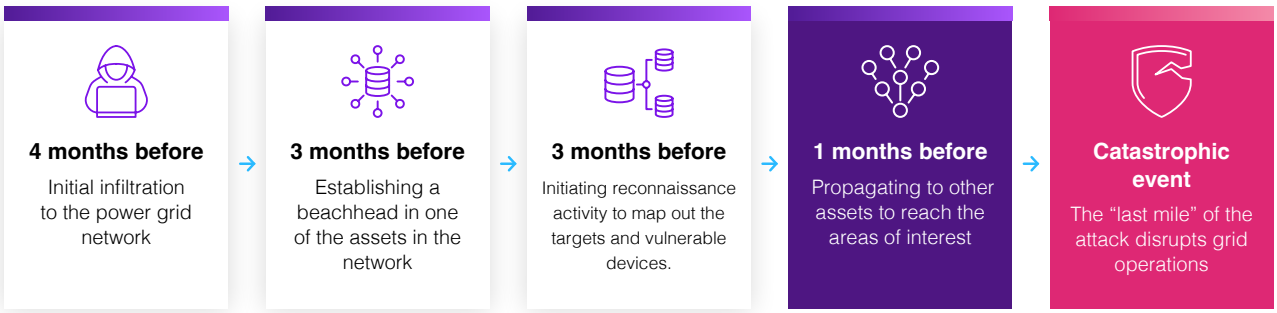
The global population is growing, and so too is the demand for energy, oil, gas, green alternatives and clean water. Having depended on legacy infrastructure for decades, the industry is facing increasing pressure to modernize and secure its networks. Digital transformation in this sector has introduced advanced technologies such as smart grids, automated meter reading, predictive maintenance, and artificial intelligence. These innovations have improved efficiency, reduced operational costs, and enhanced service delivery. Of course, this has introduced a wave of connected assets and a rapidly expanding attack surface. The utilities sector now generates vast amounts of data, which must be strategically managed to ensure operational resilience and security.

The energy sector is becoming an increasingly attractive target for cybercriminals and even state-sponsored cyberattacks. Colonial Pipeline may have happened in 2021 but its impact is still widely spoken about—a six-day shutdown of critical oil infrastructure. It's incidents like these that have exposed the vulnerabilities in the energy sector. Recent attacks have shown that little has been done to control the situation or recognize the urgency.

In response, energy companies have ramped up investments in cybersecurity companies in a bid to get ahead of the curve. Although investment is lower than during the 2021 boom, investment in 2024 has already more than doubled compared to the previous year, reflecting the industry's commitment to strengthening its defenses.

Anatomy of a Cyber Attack in the Energy Sector

Here's the breakdown of what an attack typically looks like. Infiltration and the initial lateral creep from IT across to your OT networks takes months. A security solution that considers this and understands preventative action can be the difference between effective mitigation and firefighting.



© Copyright Armis 2025

OT Examples in Energy and Utilities:

- **Power Generation:** OT systems control critical processes such as turbine operation, boiler management, and emissions monitoring in power plants.
- **Transmission and Distribution:** OT technologies manage the flow of electricity across vast networks, including substation automation, grid monitoring, and fault detection systems.
- **Smart Grids:** OT solutions enable real-time monitoring and management of electricity distribution, optimizing energy use and ensuring grid stability, ultimately protecting the delivery of electricity to thousands of households.
- **Water Utilities:** OT systems are integral for water treatment, distribution, and sewage management, ensuring the safe and reliable delivery of water services.
- **Gas Utilities:** OT technology controls gas pipeline monitoring, leak detection, and pressure regulation, maintaining safety and efficiency across the network.

© Copyright Armis 2025

Real-World Attacks on the Energy and Utilities Sector have been Increasing for over a Decade

On December 23, 2015, at the Prykarpattyaoblenergo power plant in Western Ukraine, a worker noticed something strange: his computer cursor was moving independently, as if controlled by an unseen hand. What he didn't know at the time was that a group of cybercriminals was behind the breach, initiating a new era of cyberattacks. In a matter of minutes, the cursor began opening circuit breakers one by one, cutting power to over 230,000 residents. The worker watched as the system logged him out, reset his password, and disabled the plant's backup generator, leaving the facility powerless.
Adecade has passed since this event, and yet many energy and utilities organizations are still surviving on the same legacy systems and managing them using spreadsheets. With political tensions rising, this sector is being targeted more than ever, here are some more recent notable attacks:

APRIL
2025

Norwegian Dam Sabotage

In a rare escalation in April 2025, Russian-linked hackers seized control of a dam in Bremanger, western Norway, fully opening its valves and releasing nearly 500 litres of water per second for four hours. The attack, attributed to a weak password, primarily affected a fish farm but spotlighted vulnerabilities in hydropower infrastructure—especially alarming given hydropower supplies over 90% of Norway's electricity.

The Guardian

MARCH
2025

Solar Inverter Vulnerabilities—Global Risk

This year security researchers uncovered 46 new critical vulnerabilities across solar inverter models from major manufacturers Sungrow, Growatt, and SMA. These flaws could let attackers manipulate energy output, disrupt utility networks, exfiltrate sensitive data, or even hijack smart home systems like EV chargers. The research underscores the broader systemic risk to global energy infrastructure tied to widely deployed, internet-connected solar devices.

TechRadar

EARLY
2024

Volt Typhoon

Early in 2024, Volt Typhoon compromised information technology of multiple critical infrastructure systems, including drinking water, in the United States and its territories, U.S. officials said. Cybersecurity experts believe the China-aligned group is positioning itself for potential cyberattacks in the event of armed conflict or rising geopolitical tensions.

CISA

© Copyright Armis 2025

Why Are Energy and Utilities Environments Targeted More Year on Year?

Geopolitical Motivations

State-sponsored cyberattacks target critical infrastructure, including utilities and electric grids, as part of broader geopolitical strategies. These attacks aim to disrupt the economic stability of adversaries, serving as a form of economic warfare.

Increased Digitization and the Convergence of IT/OT

Enhancing efficiency and connectivity has come at a cost. The convergence of IT and OT systems has expanded the attack surface for cybercriminals. Compromising one system can often grant access to others, making these sectors attractive targets for cyber threats.

High-Impact Ransomware Attacks

Attacks on critical infrastructure can cause widespread disruption, making them lucrative targets for cybercriminals. The ability to disrupt power supply, contaminate water, or compromise gas pipelines increases the likelihood of ransom payments and media attention.

Economic Incentives

The utilities sector is vital to the global economy, with any disruption having cascading effects on industries and consumers. Cybercriminals exploit this vulnerability, knowing that companies might be more willing to pay ransoms to quickly resume operations.

Vulnerability of Legacy Systems

Many utilities still rely on legacy OT systems that were not designed with cybersecurity in mind. These outdated systems often lack modern security features, making them easier to exploit and challenging to secure in an interconnected environment.

© Copyright Armis 2025

An end-to-end Solution - The Centrix™ Platform

Securing Energy and Utilities Organizations in 5 Steps

1. Flexible Hybrid Deployment

Meeting the Needs of Critical Infrastructure

Every energy and utilities environment is unique. Some require strict on-premise control of data due to regulatory mandates, while others need the agility and scalability of SaaS to enable real-time functionality and faster threat detection. Armis recognizes this duality and provides flexible deployment options that align with the realities of critical infrastructure.

With **on-premise deployment,** organizations can keep sensitive operational data within their own environment, ensuring compliance and peace of mind. **SaaS deployment** delivers always-up-to-date intelligence, real-time analysis, and faster remediation capabilities. Many utilities benefit from a **hybrid approach**, leveraging on-premise for data sovereignty while enabling SaaS for proactive threat detection and accelerated response.

This flexibility allows utilities to adopt a deployment model that matches their operational, regulatory, and security requirements without compromise, ensuring resilient protection across their IT, OT, and IoT assets.

2. Visibility

Armis Centrix™ Secures the Entire Lifecycle of Your Assets

As the Energy and Utilities sector becomes more complex, the need for seamless integration and coordination between diverse systems is paramount. This complexity requires infrastructure that is not only intelligent but capable of real-time tracking and coordination of a broad range of assets. To achieve real-time operational capabilities and swiftly adapt to changes, these systems must be interconnected, both among themselves and with the internet.

In this context, ensuring the visibility, security, and control of your OT infrastructure is vital for reliable and efficient operations. Armis understands the unique challenges faced by the utilities sector. Armis Centrix™ offers comprehensive end-to-end services, from proactive mitigation with Early Warning Capabilities to Vulnerability Prioritization designed specifically for OT environments. With Armis Centrix™ for OT/ IoT security, utilities can proactively protect against threats and minimize disruptions.

Complete Visibility Across the Entire Network

In utility environments, numerous systems must work in perfect synchronization for successful operations. For example, in a power plant, OT systems manage critical processes like turbine operation and grid stability. Any disruption can lead to power outages, with widespread effects. The systems that make all this happen rely on a converged IT/OT infrastructure. Complete 360-degree visibility across the entire infrastructure ensures there are no security blind spots that can potentially disrupt or disable operations. Visibility must be at the network level to identify questionable or anomalous traffic, and at the device level to find infected devices that may or may not communicate on the network.

© Copyright Armis 2025

3. Proactivity

Proactive Threat Management

Leveraging AI technologies for proactive threat detection, Armis employs sophisticated algorithms and machine learning with its Asset Intelligence Engine to identify and respond to cybersecurity threats in real-time. This advanced capability enables the preemptive recognition and mitigation of sophisticated cyberattacks that traditional security tools might miss.

Armis Centrix™ for Early Warning is revolutionizing how utilities proactively understand and mitigate risk. Armis provides a comprehensive view of industry events, allowing organizations to stay ahead of potential risks. With human intelligence, smart honeypots, and state-of-the-art research, Armis Centrix™ ensures timeliness, unparalleled coverage, and accuracy, enabling organizations to stay ahead of evolving cyber threats and protect their critical assets with confidence.

Heard of Armis Labs?

Check out the home of all Armis discovered vulnerabilities at www.armis.com/armis-labs/. See the CVEs that are targeting your industry and prioritize your own patching efforts accordingly.

4. Bespoke Management

Secure Remote Access for Essential Third Party Maintenance

More so than other OT industries, energy and utilities locations can be difficult to access, remote and dispersed. From a wind farm out in the ocean or a nuclear plant specifically built away from infrastructure or by the water for cooling reactor cores. Secure remote access is the only viable way to get the necessary maintenance done to your environment. With Armis, our Secure Remote Access is Policy Driven and focuses on enabling just in time access so your network is open to third parties for a minimal period of time.

Network Segmentation and Policy Enforcement

By providing comprehensive visibility into connected assets and their communications, Armis can segment or recommend network segmentation policies that are automatically enforced via existing firewalls and network access control (NAC) solutions. This ensures critical systems are isolated from potential threats, enhancing overall cybersecurity resilience.

© Copyright Armis 2025

Manage Dispersed OT Assets Proactively to Minimize the Attack Surface Continuously

Governance requires an array of options for swift mitigation or remediation, as well as knowing which option to use based on all available intelligence. Armis automates response workflows, including SIEM/SOC incident response and dynamic segmentation, to protect high-risk networks and keep mission-critical assets online.

5. Risk Prioritization

Addressing Vulnerabilities and Other Security Findings Effectively Armis Centrix™ for VIPR Pro – Prioritization and Remediation in the Energy and Utilities Industry

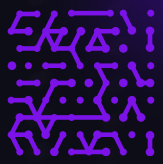
Utilities are overwhelmed by security alerts without a scalable way to prioritize or remediate them, but Armis Centrix™ offers a comprehensive solution by consolidating security findings across all sources and automating prioritization. It specifically addresses the challenges posed by SCADA systems, which are critical for monitoring and controlling industrial processes. By unifying asset knowledge from complex OT environments, including SCADA systems, and leveraging AI-driven remediation capabilities, it enables data ingestion from various sources while reducing findings volume through ML deduplication. Contextualizing findings with threat intelligence and operational impact allows for prioritized fixes based on business significance and likelihood of exploitation. Additionally, Armis Centrix™ streamlines ownership assignment for remediation, integrates with existing workflows, and simplifies tracking progress in OT environments through a consolidated dashboard, ensuring effective risk resolution and continuous improvement.

Take Aways

OT cybersecurity is now recognized as a critical component in ensuring a reliable, efficient, and safe utility environment. To mitigate associated risks, full visibility, security, and control over operational assets are imperative. Armis delivers comprehensive visibility across both IT and OT assets, with deep situational analysis down to the firmware and backplane level.

Proactive threat hunting strategies identify weak points before potential threat actors can exploit them. Vulnerability management prioritizes vulnerabilities with known exploits pertinent to your specific environment. Network controls meticulously track and document any changes made to your OT infrastructure, enabling auditing and rollback when necessary. Armis's flexible deployment options and integration with leading IT security vendors ensure that utility infrastructures operate with enhanced safety and reduced risk.

© Copyright Armis 2025



ARMIS®

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo

© Copyright Armis 2025