Zero Trust OT Cybersecurity Protection for the Energy Industry

Power is the lifeblood of the modern world, ensuring the flow of energy that powers homes, businesses, and industries. BlastWave understands the critical role energy network administrators play and the immense responsibility they shoulder in protecting this essential infrastructure. Our Zero Trust solutions are specifically designed to fortify energy OT networks against sophisticated cyber threats, eliminating the root causes of attacks and providing resilient security for the most vital operations, from power generation to oil and gas production. We empower energy companies to maintain uninterrupted energy delivery, safeguard their assets, and ensure the safety and well-being of communities.

Energy companies face unique and critical cybersecurity challenges, given the essential nature of their services and the potential for devastating consequences from cyberattacks. They also face the challenge of complying with indistry standards like NERC CIP.

Energy customers choose us to protect their OT network because BlastWave uniquely:

Protects Critical Infrastructure: Safeguard essential systems like power plant control systems, pipeline SCADA, and refinery automation, preventing damage and ensuring operational continuity.

Secures Remote Operations: Enable secure remote access for monitoring and control of geographically dispersed assets, improving efficiency without compromising security.

Aids in Compliance with Regulations: Helps energy companies meet industry-specific cybersecurity regulations, such as NERC CIP, and avoid penalties.

Protects Against Advanced Threats: Network cloaking , software-defined segmentation, and passwordless MFA effectively counter sophisticated AI-driven reconnaissance and phishing.

BlastShield

Prevention of Service Disruptions: Minimize the risk of cyberattacks that could disrupt power generation, ensuring reliable energy delivery to customers.

Enhanced Safety: Protect against attacks that could lead to safety hazards, such as power plant explosions, pipeline leaks, or industrial accidents.

Protection of Legacy Systems: BlastWave provides a "virtual air gap" for vulnerable legacy equipment that cannot be easily patched, mitigating the risk of exploitation.

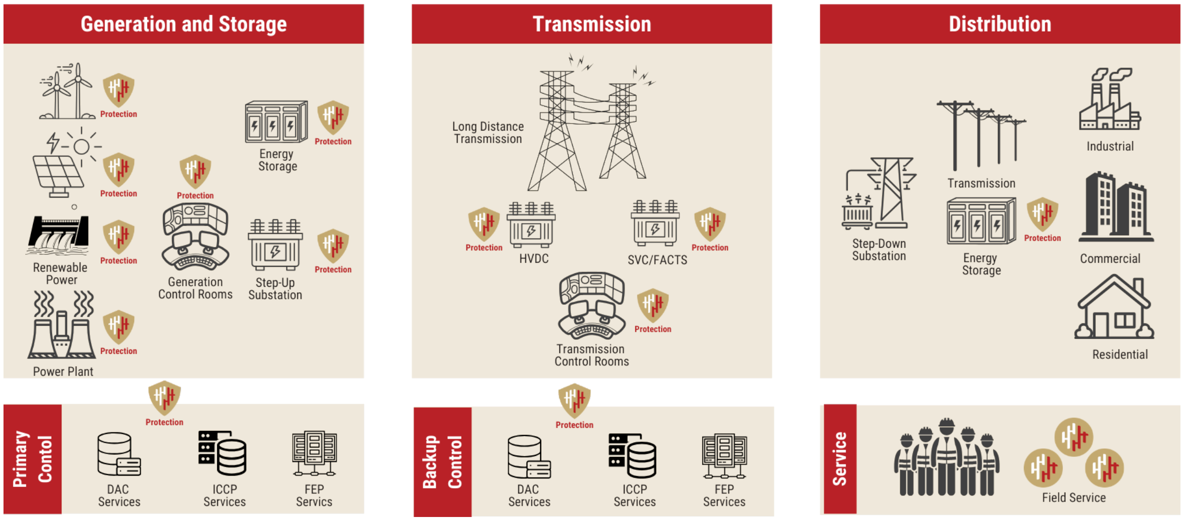

Figure 1 BlastWave in Energy Networks

BlastShield™: Zero Trust OT Protection for Energy Industry Systems

BlastWave delivers exceptional value to energy OT networks by fundamentally changing how security is approached. We move beyond traditional perimeter defenses that are increasingly ineffective against modern cyberattacks. Instead, we implement a robust Zero Trust architecture that eliminates the root causes of vulnerabilities. This includes network cloaking, which renders critical energy systems invisible to attackers, preventing reconnaissance and reducing the attack surface. We also employ passwordless multi-factor authentication (MFA), thwarting phishing and credential theft, a major source of breaches. Finally, our software-defined segmentation allows for granular control, limiting lateral movement and containing the impact of any successful intrusion.

This comprehensive approach provides a more secure and resilient foundation for energy operations. By proactively addressing the weaknesses that attackers exploit, BlastWave minimizes the risk of disruptions, protects valuable assets, and ensures the safety and reliability of energy delivery. This is crucial for maintaining the stability of power grids, preventing oil and gas pipeline incidents, and safeguarding renewable energy infrastructure. Ultimately, BlastWave empowers energy companies to operate with greater confidence and efficiency in an increasingly complex and threatening cyber environment. BlastWave use cases for the energy industry include:

Power Generation (Nuclear, Fossil Fuel, Renewable):

Securing Control Systems (DCS, SCADA):

BlastWave protects critical control systems from unauthorized access and manipulation. Zero Trust technology is used to protect from both remote and local threats, including the use of segmentation to protect against malicious insiders. This protection prevents disruptions to power generation and potential safety hazards and enables secure remote monitoring and control of power plants.

Protecting Substations and Transmission Lines:

Securing remote substations and transmission lines from cyberattacks is a key link in the energy supply chain. These remote sites require a solution designed for OT environments to prevent disruptions to power distribution and grid stability and to Enable secure remote maintenance and monitoring when power and space are at a premium for security.

Securing Renewable Energy Sites (Wind, Solar):

Clean energy sites are often in remote sites with highly variable network connections, but still require a secure infrastructure that can protect control and monitoring systems. BlastWave secures the data connections used for data acquisition and transmission from remote sites.

Protecting Legacy Systems:

Protecting legacy systems with a virtual air gap to prevent exploitation of unpatchable OT systems ensures that vulnerable systems do not fall victim to known and zero-day exploits.

Securing Smart Grid Infrastructure:

Smart meters, communication networks, and grid management systems require secure data flows to prevent manipulation of grid operations.

General Energy Use Cases:

Secure Remote Access:

BlastWave's passwordless MFA enables secure access for employees, contractors, and vendors, facilitating remote maintenance, troubleshooting, and operations while preventing credentials theft.

Threat Prevention:

Network cloaking and software-defined segmentation protect against ransomware, malware, and phishing attacks by making OT networks undiscoverable, preventing denial-of-service attacks, and leveraging zero trust to prevent intrusions and lateral movement.

Regulatory Compliance:

BlastWave is a key component in meeting regulatory requirements (NERC CIP, etc.) and building a secure infrastructure in line with NIST secure architectures and risk management models.

BlastShield's unique combination of AI-Resistant Network Cloaking, Phishing-Resistant Secure Remote Access, and Software Defined Segmentation ensures energy providers can secure their networks in accordance with numerous industry-specific requirements and keep their infrastructure resilient and operational. Keeping the power on is paramount, and BlastWave is here to help energy companies build secure infrastructure for their consumers.

v20250409

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

**1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499**