SOLUTION BRIEF

AI-Resistant Cybersecurity Protection for Energy

The Operational Technology Challenge for Energy

The energy industry plays a critical role in powering our economy, supporting every essential service for society. This criticality makes it an attractive target for bad actors and cybercriminals who seek to disrupt it for financial gain, reputational damage, or to cause chaos.

The escalating threats from hacking pose an immediate danger to national energy infrastructures. These threats have rapidly escalated as AI-powered hacking tools have dramatically improved even novice hackers' ability to conduct reconnaissance and craft targeted phishing lures toward energy networks.

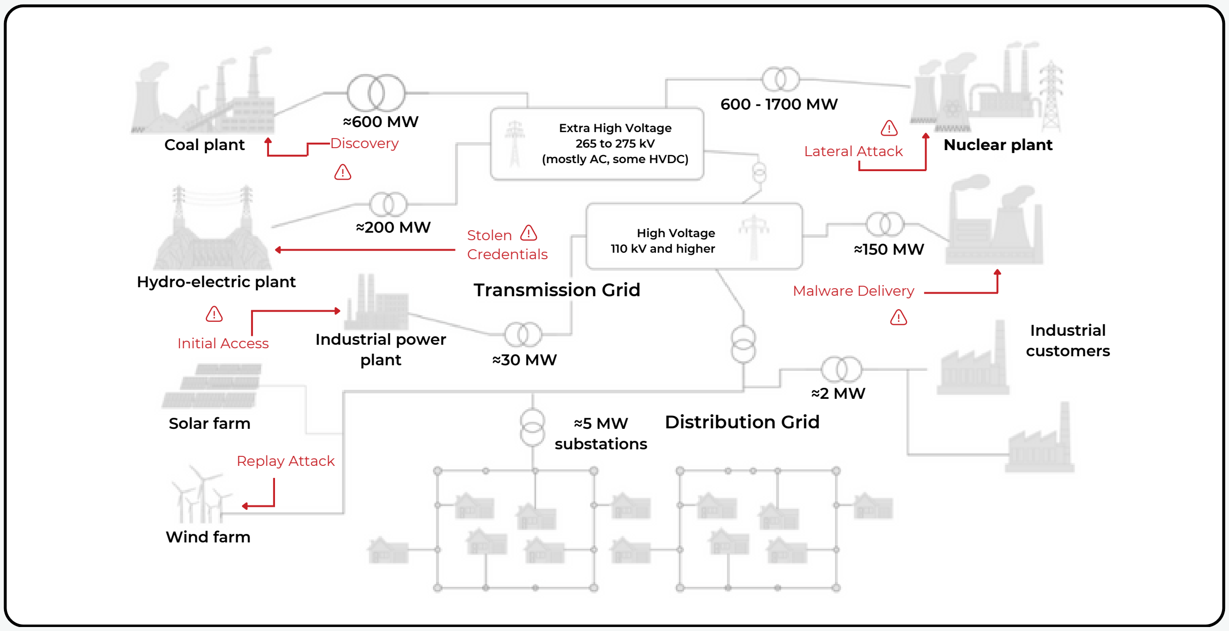
The industry has created regulations like NERC CIP and IEC 62443, which require energy providers to operate more secure networks. The challenge is that existing IT-oriented security solutions do not provide adequate security in this new AI-enabled cybersecurity landscape. Edge-to-cloud applications, IoT, and the hybrid workforce have made perimeter-based approaches like VPNs, firewalls, and VLAN segmentation obsolete.

Energy networks need an AI-resistant solution deployed within their existing OT environment that is easy to use for their administrators and users.

BlastShield Advantages:

- Reconnaissance-Proof Software Defined Perimeter to prevent device discovery and vulnerability exposure with Network Cloaking
- Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- Delivers Least Privilege Access Policies and prevents Lateral Movement with Network Microsegmentation

Figure 1: Potential Cyber Threats to an Energy Infrastructure



BlastShield™: AI-Resistant OT Security For Energy

BlastShield is an ideal solution to help energy networks achieve regulatory compliance, as it is easily deployed as a simple migration without any changes to the existing IT or OT network architecture. Installing and administering the solution takes an order of magnitude less time and effort than comparable solutions. The user experience is comparable to Apple Pay, with simple biometric authentication granting access to only the devices the user needs.

BlastShield provides a PKI-authenticated secure gateway to the OT environment, where Industrial control systems, PLCs, IEDs, RTUs, turbine controllers, valves, and IoT devices remain in service for decades, long after vendors halt support. These systems often cannot be patched but require access to internal monitoring systems. BlastShield protects these systems from discovery by hackers by creating a virtual air gap with Network Cloaking, Only allowing biometric-authenticated Secure Remote Access to the devices and leveraging Network Segmentation to create microsegmentation of different device types to prevent lateral movement within an existing flat Layer 2 network.

Network Cloaking

BlastShield's network cloaking provides a first line of AI-resistant security by preventing reconnaissance and breaking the cyber kill chain. It proactively secures systems, making them invisible to potential attackers by blocking all internet access for legacy OT systems. Imagine a hacker scanning a network for surveillance and finding nothing. Valuable OT assets, from Human-Machine Interfaces (HMIs) to essential workstations, vanish from security scans. Network cloaking also creates a virtual air gap for OT systems that do not need access to the internet by only allowing them a hidden private IP address. As the cybersecurity landscape evolves and threats become more advanced, adopting network cloaking isn't just a tactical move; it's a strategic necessity with many legacy systems that will never be patched.

Secure Remote Access

BlastShield provides AI-resistant secure remote access, employing a solid combination of multi-factor authentication (MFA), biometrics, and AES-256 encryption to prevent attacks from breaching our outer defenses. The MFA techniques resist phishing attacks with biometrics and other authentication factors, providing a more secure defense against AI-powered threats. A mesh of P2P tunnels delivers end-to-end protection from the initial login to the final data transmission; all interactions within the BlastShield utilize AES-256 encryption and meet regulatory requirements for data protection.

Network Segmentation

BlastShield exceeds traditional segmentation by advancing the concept of microsegmentation as a superior security alternative. Unlike broad segmentation strategies, microsegmentation allows for incredibly detailed control, segmenting networks down to the level of individual devices, systems, protocols, or users. By isolating network segments, BlastShield effectively prevents the lateral movement of threats within the network, a critical defense mechanism against external and internal threats. Policy changes take effect in real time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments. With its detailed segmentation capabilities, BlastShield aids in compliance with stringent regulatory standards, offering necessary tools to protect sensitive data and ensure privacy. BlastShield's microsegmentation solution is innovative, future-ready network security.

About BlastWave

BlastWave prevents AI-powered cyber attacks on critical infrastructure with a unique combination of Zero Trust Cybersecurity capabilities and delivers industrial-grade security with consumer-grade ease-of-use. Visit www.blastwave.com to learn more