

BlastShield Introduction

Securing Europe's Critical Infrastructure Against Dormant Threats

The European energy and power industry is the foundation of the continent's economy and security. However, the biggest threat to this infrastructure is not just future attacks, but the malware and rogue components already embedded within existing networks. Entire industry and service sectors are known to have been compromised by state and non-state actors who are simply waiting to send commands to damage, switch off, or otherwise compromise critical infrastructure.

Traditional IT security is ill-equipped for this reality and the unique challenges of OT environments. A new, purpose-built approach is needed to protect essential networks from both external attackers and the manipulation of these pre-existing, dormant threats. BlastShield™, developed by the US company BlastWave, is a very cost-effective way to protect infrastructure, including energy infrastructure, from these threats, by providing an "overlay" (or "cloaking") to protect all systems from internal and external threat, without needing to alter existing IT and OT systems.

At BlastWave, we are pioneering a transformative approach to cybersecurity that fundamentally enhances the protection of critical infrastructure. Our flagship solution, BlastShield, offers unmatched defense against the very types of cyber threats that target thermopower, hydropower, electricity grids, PV solar, battery storage, wind power, district heating, and natural gas transmission and storage.

Protecting operational technology requires a specialized approach to avoid significant service disruptions and financial consequences. Relying on traditional IT-centric firewalls can introduce further challenges, including escalating complexity, costly administration, and a higher potential for security misconfigurations. BlastShield is engineered to prevent these issues with a cost-effective and non-disruptive solution. As a secure software overlay, it deploys in hours without altering the existing network, eliminating the downtime and intricacy of hardware-based projects. This radical simplicity allows BlastShield to deliver superior protection at approximately one-quarter the cost of competing cyber-defense solutions.

What is BlastShield™?

An Overlay Cyber-Defense Perimeter

BlastShield™ is an overlay cyber-defense software perimeter designed to protect critical infrastructure. Because BlastShield™ is an overlay network, it can be deployed without removing or replacing any pre-existing security products. It is engineered from the ground up to address the core vulnerabilities of OT and SCADA environments. Its effectiveness is founded on three Zero Trust principles:

- 1. Network Cloaking:** BlastShield™ makes your entire OT network invisible to unauthorized users by cloaking all network addresses with its own generated IP addresses. This makes underlying assets invisible to hackers scanning from the outside. This "cloaking" mechanism reduces the number of attacks to near zero – a fact that is easily demonstrated



BlastShield Features

- Phishing-resistant MFA authenticates the remote pilot-in-command before connection
- Device cloaking that hides the public IP address and web services of the aircraft, control stations and cloud servers
- Simple orchestration replaces complex PKI and firewall management
- On-premises Orchestrator for air-gapped networks

with Red Team penetration exercises. If an attacker cannot see their target, they cannot attack it.

- 2. Passwordless Authentication:** Over 60% of network breaches occur because of stolen usernames and passwords. BlastShield™ eliminates this attack vector by removing username and password authentication entirely. The only options for access are phishing-resistant and strong, such as biometric authorization on a mobile phone paired with a laptop or FIDO keys.

3. Auto-Segmentation: BlastShield™ makes the notion of a “flat network,” where any hacker or insider can roam wherever they want, a thing of the past. It enables auto-segmentation, allowing network managers to create secure micro-perimeters around critical assets and isolate groups of endpoints from one another. These segmentation changes are done with the flick of a switch in seconds, rather than over hours or days.

Neutralizing Embedded Threats

The most critical feature of BlastShield™ is its ability to prevent the manipulation of malware or “rogue components” already present in a network when it is turned on. BlastShield™ prevents these embedded threats from sending or receiving commands to or from agents outside the network, effectively neutralizing them.

It is important to know that BlastShield™ does not scan for or detect suspicious activity. It focuses purely on protection. For this reason, asset discovery and monitoring tools from companies like Dragos and Nozomi are often deployed alongside BlastShield™. While they identify anomalies, BlastShield™ neutralizes the threats – known or unknown – allowing security teams to eliminate them at their leisure.

Proven Success in Demanding Environments

- **BlastWave’s effectiveness:** Proven in some of the world’s most security-conscious environments:
- **Global Industrial Deployments:** BlastWave protects over 5,000 industrial control sites across 13 countries.
- **United States Department of Defense (DOD):** Our solution is successfully deployed to protect critical infrastructure at U.S. military installations, including Spangdahlem Air Base in Germany and Arnold Air Force Base.

The BlastWave Advantage: A Paradigm Shift in OT Cybersecurity

- **Superior Security:** A proactive Zero Trust approach stops breaches before they start and neutralizes embedded malware.
- **Radical Simplicity and Speed:** BlastShield™ is an overlay that does not require you to shut a network down, add or replace hardware, reboot, or reconfigure it. Once endpoints are catalogued, BlastShield™ can be stood up and made operational within hours.
- **Reduced Costs:** As a 3-in-1 software solution, BlastShield™ costs on average one-quarter as much as other cyber-defense products and traditional firewall projects.
- **Protection for Legacy Systems:** Our “virtual air gap” technology protects older, un-patchable devices without requiring costly and disruptive upgrades.

v20260330

Prevent industrial cyberattacks, and ensure the world’s critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at www.blastwave.com

©2025 BlastWave Inc. | 1045 Hutchinson Ave., Palo Alto, CA 94301 USA | T: +1 650 206 8499

