S&P Global
Market Intelligence

Coverage Initiation: BlastWave elevates OT security with BlastShield zero-trust overlay for critical infrastructure

Analysts - Johan Vermij

Publication date: Thursday, December 11 2025

Introduction

Operational technology networks face pressure from ransomware, AI-assisted reconnaissance and credential compromise techniques. Network segmentation and VPN access models struggle to protect legacy industrial control systems, supervisory control and data acquisition tools, flat networks, and pervasive remote access.

BlastWave positions its BlastShield platform as a zero-trust overlay that renders assets invisible, enforces phishing-resistant access and segments east-west traffic without requiring major network redesign. It emphasizes blocking the reconnaissance and credential theft phases of the cyber "kill chain," arguing that 95% of breaches exploit reconnaissance and credential compromise. With partners in the asset visibility space, as well as a target market spanning small utilities to large oil and gas operators, BlastWave is seeking to simplify and scale OT security via its overlay model.

The Take

The vendor's BlastShield platform represents a strategic response to the evolving threat landscape in the OT category. By shifting the security paradigm from reactive detection to proactive invisibility and human-centered authorization, BlastWave addresses the root cause of many OT breaches — reconnaissance and credential compromise. Its overlay architecture and cost-efficient licensing make BlastWave particularly suited for brownfield and midtier industrial sites, where traditional cybersecurity controls are often lacking. As ransomware and AI-driven attacks in the OT segment escalate, the ability to make critical assets invisible and accessible only through authenticated human-in-the-loop permission offers meaningful risk reduction. For organizations looking to secure

legacy and distributed OT networks with minimal disruption, the company represents an alternative to traditional firewalls and VPNs to achieve industrial cyber resilience.

Context

Palo Alto-based BlastWave was founded in 2017 by executives with backgrounds at Apple Inc. and Google. Its leadership team includes cofounder and CEO Tom Sego, CTO Peter Alm, and other security veterans. The vendor has raised roughly $10.3 million in funding, including an $8 million series A round in October 2018, according to Capital IQ Pro. The series A was led by Rocket Strategies, with participation from Don Lucas Ventures and Millennium Investments. BlastWave has engineering and sales teams located in the US, Europe and the Middle East. Its strategic partnerships, most recently with UTSI for OT cyber resilience, further extend its reach into mission-critical infrastructure sectors.

Technology

BlastShield implements a software-defined perimeter purpose-built for OT environments, replacing or reducing reliance on traditional firewalls, VPNs, access control lists, privileged access management systems, SDN configurations, and jump hosts. At its core, the platform combines three capabilities: network cloaking, passwordless phishing-resistant multifactor authentication (MFA), and software-defined micro-segmentation. Its overlay-based segmentation is central to its architecture.

Instead of modifying IP addresses, variable-length arrays or physical network topology, BlastShield creates a secure overlay that renders OT assets invisible to unauthorized users and scanning tools. This makes it suitable for brownfield deployments where re-architecting networks is impractical and where legacy systems often depend on fixed IP configurations. Access control is built around a human-in-the-loop model. BlastWave enforces identity verification using passwordless, phishing-resistant MFA paired with device binding, ensuring that access is tied to both a known user and a known device. In this model, authentication relies on "something you have" and "something you are," rather than passwords or knowledge-based factors.

Strategically, the vendor focuses on preventing reconnaissance and credential compromise, which it argues are the dominant precursors to OT breaches. By cloaking devices and eliminating exploitable credentials, BlastShield aims to break the early stages of the kill chain. It claims that this proactive approach is more effective than detection-centric or malware-driven defenses, especially as attackers increasingly employ AI-assisted scanning and automated exploitation.

The platform integrates with visibility vendors such as Dragos, Nozomi Networks and Phosphorus for asset discovery and threat intelligence. This allows BlastShield to ingest Microsoft Active Directory users, asset and device lists, as well as feed outputs into security information and event management (SIEM) systems such as Splunk and IBM QRadar to facilitate operationalization. Whereas many security tools come with a price tag too big for smaller enterprises, BlastWave's pricing and economics appear to fit smaller sites, bringing it in range for small utilities, wastewater lift stations, or single well-heads in the oil and gas industry. Endpoint-level licensing starts at $30 per protected endpoint, or networks for as little as $300.

Competition

While most investments in OT security over the past decade have gone to asset visibility specialists, there is a growing number of companies focused on secure remote access, network cloaking and network segmentation in OT environments. BlastWave vies with OT specialists and broader enterprise security providers. On the OT-focused side, rivals such as Cyolo, Xage

Security and Xona Systems offer zero-trust or secure remote access, and players like Elisity and Illumio provide micro-segmentation for industrial networks.

A third set of vendors that BlastWave encounters includes Invisinet, Opscura, Tempered Networks and others that offer OT network cloaking technology. Traditional industrial automaton/OT incumbents like Siemens AG (via its SINEC Secure Connect platform) and Schneider Electric SE are also extending their portfolios into OT zero-trust access and segmentation. On the enterprise side, companies such as Cisco Systems Inc. (Duo/AnyConnect), Fortinet Inc., Palo Alto Networks Inc., Zscaler Inc. (Private Access), CyberArk Software Ltd., BeyondTrust and Delinea are migrating into the OT space as well.

SWOT Analysis

Strengths	**Weaknesses**
BlastWave offers a lightweight, overlay-based zero-trust platform that can retrofit existing OT environments without major network changes. Its emphasis on blocking reconnaissance and credential attacks aligns with current threat trends in the OT category such as ransomware increases. The company's cost-accessible licensing model targets small utilities and distributed sites, broadening its addressable market.	Being smaller than major cybersecurity or automation providers could limit BlastWave's global go-to-market reach, ecosystem depth and integration breadth. Its overlay-only approach could still require convincing customers to migrate from traditional perimeters. Moreover, its operational proof points at scale could be fewer compared with legacy cybersecurity players.
Opportunities	**Threats**
A surge in OT ransomware (up roughly 87% year over, according to BlastWave) and increasing regulation across critical infrastructure offer strong tailwinds. Demand from smaller utilities, decentralized energy systems and remote OT sites presents a sizable addressable segment. The vendor's ability to partner with visibility vendors and integrate with SIEM specialists positions it for broader service offerings.	Large enterprise/security vendors are rapidly entering the OT zero-trust category — as such, consolidation could raise the competitive pressure. Legacy OT inertia and budget constraints could slow adoption. Attackers might evolve tactics beyond reconnaissance/credential theft or focus on supply-chain or model-based attacks that circumvent perimeter/overlay protections.

Source: 451 Research.