Security and Visibility for OT

Operational technology (OT) environments face a unique and growing set of security challenges. OT systems often rely on proprietary protocols, are filled with decades-old legacy devices that cannot be patched, and have an unwavering priority on safety and uptime over everything else. The increasing convergence of IT and OT networks has exposed these vulnerable systems to modern cyber threats, including sophisticated ransomware, supply chain attacks, and state-sponsored espionage.

A Combined Nozomi Networks/BlastWave Solution: See, Secure, and Control

The Nozomi Networks and BlastWave combined solution offers a unified and non-disruptive approach to OT cybersecurity. This powerful partnership bridges the gap between passive monitoring and proactive enforcement, providing the clarity to see every threat, the power to secure every connection, and the control to contain any breach.

Nozomi Networks acts as your eyes and ears, providing unmatched visibility into your entire OT, IoT, and IT environment. Its deep packet inspection and AI-powered analytics passively discover every asset, map network communication, and detect anomalies or threats in real-time – all without impacting your critical operations.

BlastWave acts as your active shield, leveraging its Zero Trust architecture to proactively secure and harden your environment. It cloaks vulnerable assets from discovery, eliminates password-based risks, and uses software-defined microsegmentation to enforce granular, least-privilege access, ensuring that even if a threat gets in, it can't move.

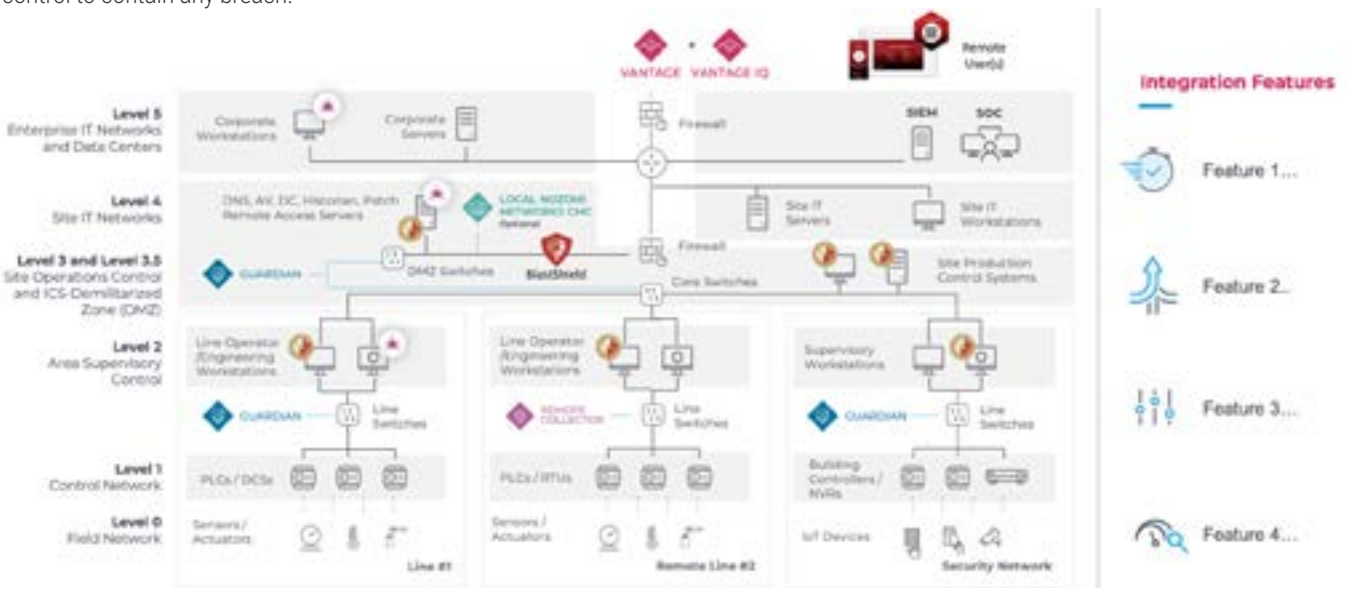
Together, these two solutions create a layered defense that first understands the environment and then secures it from the inside out.

Joint Solution Advantages

Automatic discovery and import of devices: Nozomi Networks automatically discovers all assets, providing a comprehensive, real-time inventory and network map that can be imported into the BlastShield orchestrator for policy-controlled device groupings.

Safely and securely automate response in OT: Leverage Nozomi's detection capabilities with BlastWave's microsegmentation policies to mitigate risks for high-risk devices.

Achieve scale for OT security: Remove scalability as a challenge by combining Nozomi's device discovery and categorization with BlastWave's policy groups to enable security policies that scale to millions of devices, unlike ACL solutions.



Protection for OT networks is not just a possibility but a reality

Key Features

Unmatched Asset Visibility and Intelligence: Nozomi Networks automatically discovers all assets, providing a comprehensive, real-time inventory and network map. It identifies device types, firmware, protocols, and vulnerabilities, giving you the context you need to understand your security posture.

Zero Trust Microsegmentation: BlastWave's software-defined zones and conduits allow you to create a "virtual air gap" and contain threats by restricting lateral movement. This granular segmentation isolates critical systems and ensures that a compromise on one device cannot spread to the rest of the network.

Proactive Attack Surface Reduction: BlastWave's unique network cloaking technology makes your most vulnerable and unpatchable legacy devices completely invisible to unauthorized users and network scans. If an attacker can't see the target, they can't attack it.

Real-Time Threat and Anomaly Detection: Nozomi Networks provides continuous monitoring for cyber threats, malicious activity, and operational anomalies. It uses a robust threat intelligence feed and AI-based analytics to identify security incidents and process deviations before they cause harm.

Secure, Passwordless Remote Access: BlastWave eliminates the weakest link in the security chain (passwords) by providing passwordless, phishing-resistant multi-factor authentication (MFA) for all remote access. This ensures that third-party vendors and internal staff can access only the specific devices they are authorized to see, for a limited time.

Automated Threat Containment: When Nozomi Networks detects a malicious threat or anomalous behavior, it can trigger an automated policy in BlastWave to instantly isolate the affected device or segment. This rapid, policy-based containment prevents the threat from spreading before it can impact operations.

Simplified, Non-Disruptive Deployment: Nozomi's passive monitoring can be implemented without causing downtime or impacting network traffic, and BlastWave's software-defined architecture eliminates the need for expensive, complex firewalls and network redesigns.

Key Benefits

Eliminate Blind Spots and Reduce Risk: Get a complete, accurate, and continuously updated view of your entire OT network. With Nozomi Networks' deep visibility, you can eliminate security blind spots and prioritize remediation efforts based on actual risk.

Contain Threats and Prevent Lateral Movement: Stop threats in their tracks. By combining Nozomi Networks' real-time detection with BlastWave's microsegmentation, you can automatically or manually contain threats within a small zone, preventing them from spreading across the network and causing widespread damage.

Protect Unpatchable Legacy Systems: Secure your critical, end-of-life equipment without costly replacements or disruptive re-architectures. BlastWave's network cloaking and virtual air gap technology shields these devices from attack, extending their operational life safely.

Simplify Compliance and Operations: This integrated solution helps you meet critical regulatory and industry standards like IEC 62443. By providing comprehensive asset inventories, policy enforcement, and detailed audit trails, you can simplify compliance, streamline audits, and reduce administrative overhead.

Enhanced Threat and Vulnerability Management: The joint solution provides a powerful way to manage vulnerabilities and threats. Nozomi's deep asset intelligence and vulnerability data inform BlastWave's microsegmentation policies, allowing you to automatically enforce stricter access controls on vulnerable devices and protect them from exploitation, even when they ca

Improve Operational Resilience and Uptime: The ultimate goal is to keep your physical processes running smoothly. By proactively preventing attacks, rapidly detecting threats, and containing any potential breach, the combined solution protects your operations from disruption, safeguarding both revenue and safety.

Next Steps

Ready to build a more resilient and secure OT environment? Contact us today to schedule a personalized demo and learn how the combined power of Nozomi Networks and BlastWave can safeguard your critical infrastructure.

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**

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS