SOLUTION BRIEF

The Convergence of Zero Trust and Industrial Automation

BlastWave and Inductive Automation Solution Integration

BlastWave

TL:DR

This report presents an exhaustive examination of the strategic and technical integration between Inductive Automation, the creators of the pervasive Ignition platform, and BlastWave, a pioneer in software-defined Zero Trust attack prevention. The collaboration addresses the critical "connectivity paradox" of the modern industrial age: the need for unlimited access to data versus the imperative to lock down critical control systems.

Inductive Automation has revolutionized the SCADA (Supervisory Control and Data Acquisition) landscape with Ignition, a server-centric, web-based platform that acts as a universal hub for industrial data. BlastWave's flagship solution, BlastShield, integrates with Ignition to cloak Operational Technology infrastructure, providing a cryptographic, invisible, passwordless Software-Defined Perimeter (SDP) as a secure overlay on the existing network.

CONTENTS

The Crisis in Industrial Cybersecurity

The protection of industrial control systems (ICS) and operational technology (OT) has historically relied on a strategy of isolation. For decades, the "air gap" (a physical separation between sensitive control networks and corporate IT networks or the internet) was the gold standard of defense. However, the relentless drive for operational efficiency and data-driven decision-making has rendered the air gap a relic of the past.

The Convergence of IT and OT: A Double-Edged Sword

The integration of IT and OT offers immense operational benefits, allowing data to flow from the factory floor to the boardroom for real-time analysis. Yet, this convergence has significantly expanded the attack surface. Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) in critical sectors such as Oil and Gas (O&G) now face the complex challenge of safeguarding diverse, geographically dispersed, and often aging OT assets.

The primary threat vector has shifted. It is no longer just the sophisticated nation-state actor using zero-day exploits; it is the commoditized ransomware attack "leaking" from the IT network into the OT environment. Attacks are increasingly focused on energy infrastructure, with 60% of targeted attacks aimed at this sector. Furthermore, the interconnectivity of supply chains means that a failure in one facility can cascade, affecting broader supply chains 65% of the time.

The Failure of Legacy Perimeter Defenses

For the past 20 years, the industry has relied on Virtual Private Networks (VPNs) and firewalls to secure remote connectivity. While these tools were adequate for a static IT environment, they are structurally flawed for the dynamic and high-stakes world of OT.

The Vulnerability of VPNs

The VPN model is predicated on a "connect first, authenticate second" architecture. A VPN concentrator sits on the public internet, listening for connection requests. This visibility makes it a target for reconnaissance and brute-force attacks. Once a user authenticates and a tunnel is established, the VPN typically grants broad network access. If an attacker compromises a single set of credentials (often through phishing), they gain a foothold inside the trusted network, from which they can move laterally to compromise safety systems or PLCs.

Research indicates that stolen credentials and phishing were involved in almost 70% of data breaches. The reliance on passwords, even when augmented with traditional Multi-Factor Authentication (MFA), remains a critical weakness. "MFA fatigue" attacks, where attackers bombard a user with approval requests until they acquiesce, have proven effective against standard MFA implementations.

The Complexity of Firewall Management

Firewalls rely on static Access Control Lists (ACLs) based on IP addresses and ports. In a modern industrial environment, where devices are mobile and IP addresses change, managing these rules becomes a Herculean task. Misconfigured firewalls, often the result of human error during complex manual updates, are a leading cause of security breaches. The rigidity of hardware-based firewalls also stifles operational agility; commissioning a new remote access path for a vendor might take weeks of ticket processing and rule testing.

The Rise of Zero Trust Architecture (ZTA)

In response to these failures, the industry is pivoting toward Zero Trust Architecture (ZTA), as codified by NIST SP 800-207. Zero Trust abandons the concept of a trusted internal network. Instead, it operates on three core principles:

Verify Explicitly:
Always authenticate and authorize based on all available data points, including user identity, location, device health, and data classification.

Use Least Privilege Access:
Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA) to protect data and improve productivity.

Assume Breach:
Minimize the blast radius of breaches and prevent lateral movement by segmenting access based on network, user, device, and application awareness.

While the philosophy of Zero Trust is sound, its implementation in OT environments filled with legacy devices that cannot support modern authentication agents presents a significant technical hurdle. This is the precise gap that the integration of BlastWave and Inductive Automation seeks to fill.

Inductive Automation's Ignition: The Connectivity Engine

Inductive Automation has redefined the industrial software market with Ignition, a platform often described as "The New SCADA." Its architecture is fundamentally different from traditional, proprietary SCADA systems, leveraging modern IT standards (SQL, Python, HTTP/HTTPS, MQTT) to create an open, interoperable ecosystem.

The Unlimited Licensing Model and Architecture

Ignition's server-centric architecture allows for unlimited clients and tags, democratizing data access across the enterprise. The core of the system is the Ignition Gateway, a web server that manages connections to PLCs (Programmable Logic Controllers), databases, and clients.

The Gateway Network

A defining feature of Ignition is the Gateway Network. This technology enables multiple Ignition Gateways to communicate with each other over a Wide Area Network (WAN), forming a distributed system.

- Hub-and-Spoke: A central enterprise gateway connects to remote sites (spokes) and aggregates data for corporate visibility.
- Scale-Out: Workloads are distributed across multiple gateways to handle massive tag counts.
- Edge Computing: Ignition Edge gateways sit at the far reaches of the network (e.g., on a remote pump or wind turbine), providing local buffering and visualization while syncing data back to the central server via the Gateway Network.

The Security and Connectivity Challenge

What if all of Ignition's communications, servers, assets, and databases remained flawlessly in latency-free operation, yet still allowed effortless, secure remote access, all while remaining undetectable from the outside? This is what the BlastShield integration is designed to deliver for Ignition users.

Port Exposure

The Ignition Gateway listens on specific TCP ports to accept incoming connections:

- **Port 8088:** The default HTTP port for non-secure web traffic.
- **Port 8043:** The default HTTPS port for secure, encrypted web traffic (Vision and Perspective clients).
- **Port 8060:** The specialized port for the Gateway Network synchronization.

In a standard "Hub-and-Spoke" architecture, the central Hub must have Port 8060 exposed to the internet (or a WAN) so that remote Spokes can connect to it. Similarly, to allow a plant manager to view the SCADA interface on their smartphone via the Perspective module, Port 8043 must be reachable from the mobile network.

The Limitations of Standard Hardening

Inductive Automation provides a comprehensive Security Hardening Guide to mitigate these risks. The guide recommends a defense-in-depth approach:

- **Secure Communication:** Enforcing SSL/TLS (HTTPS) to encrypt data in transit and redirecting all HTTP traffic to HTTPS.
- **Identity Management:** Utilizing internal or external Identity Providers (IdP) for user authentication.
- **Network Segmentation:** Crucially, the guide advises that segmentation should be applied externally to Ignition using routers, switches, and firewalls.

Here lies the friction: managing external segmentation via traditional firewalls is complex. Opening Port 8043 or 8060 to the internet, even with SSL/TLS, exposes the web server stack to potential zero-day vulnerabilities and Denial-of-Service (DoS) attacks. The "hardened" Ignition gateway is still visible to anyone who scans the IP address.

To achieve true Zero Trust, where the gateway is invisible to unauthorized users yet accessible to authorized users, a new layer of abstraction is required. This is the role of BlastWave's BlastShield.

BlastWave's BlastShield: The Software-Defined Shield

BlastWave has developed BlastShield, a solution engineered to deliver Zero Trust Network Access (ZTNA) within the constraints of the industrial world. The systems on the OT network, like Inductive's, need access to other connected systems, often located on different network segments, to operate. BlastShield enables Ignition's communication within a secure overlay network that requires NO new firewall rules and allows all ingress rules to be REMOVED!

Software-Defined Perimeter (SDP) Architecture

BlastShield utilizes a Software-Defined Perimeter (SDP) approach. Unlike a VPN, which essentially extends the corporate network to the remote user, BlastShield makes the entire OT network, regardless of location or physical connectivity, appear as a single flat network to the systems that are allowed to communicate. Systems that are not allowed to communicate cannot even see other systems connected to the same physical network, providing the strongest security for critical infrastructure.

The "Invisibility" Cloaking Mechanism

The defining feature of BlastShield is Network Cloaking. In a traditional setup, a server responds to "knocks" (TCP SYN packets) from any IP address. BlastShield changes this behavior.

- **Drop-All Policy:** A BlastShield-protected gateway is configured with a default "drop-all" policy for inbound traffic. It does not respond to ICMP pings or unsolicited TCP requests.
- **First-Packet Authentication:** Access is granted only if the incoming packet contains a specific cryptographic authorization token. If the token is missing or invalid, the packet is silently dropped.
- **Result:** To a hacker scanning the internet with tools like Shodan or Nmap, the BlastShield-protected Ignition server does not exist. It appears as a "black hole," rendering reconnaissance, the first step of the cyber kill chain, impossible.

Passwordless Multi-Factor Authentication (MFA)

Recognizing that 80% of OT incidents start with compromised IT credentials, BlastWave has eliminated passwords from its authentication workflow.

- **Biometric Binding:** BlastShield leverages the biometric capabilities of modern smartphones (Face ID, Touch ID). The user's identity is bound to their physical device.
- **Three-Factor Security:** Access requires:
  1. **Something You Are:** The biometric scan.
  2. **Something You Have:** The registered mobile device (the authenticator).
  3. **The Device You Use:** The cryptographic signature of the laptop or client machine.
- **Phishing Immunity:** Because there is no password to type, there is no password to phish. An attacker cannot replicate the physical device and biometric signature required to initiate the connection.

Peer-to-Peer Full Mesh Performance

Traditional ZTNA and VPN solutions often rely on cloud gateways that "hairpin" traffic. A user in Dallas connecting to a server in Houston might have their traffic routed through a data center in New York, introducing latency.

- **BlastShield Architecture:** BlastShield establishes a full-mesh peer-to-peer network. The orchestration plane (in the cloud) brokers the connection, but the data plane (the actual traffic) flows directly between the user and the resource.
- **Performance Benchmark:** Independent testing by the Tolly Group verified that BlastShield performs up to 34x faster than competitor solutions. This low-latency performance is critical for SCADA applications that require real-time control.

Technical Integration: Integrating BlastWave with Ignition

The integration of BlastShield with Ignition does not replace Ignition's internal security; rather, it wraps the entire architecture in a secure, invisible envelope. BlastWave is a recognized member of Inductive Automation's Technology Ecosystem Program, ensuring that the solution has been validated for compatibility and value.

Deployment Topologies

BlastShield can be deployed in two primary configurations to protect Ignition environments: the Agent Model and the Gateway Model.

The Agent Model (Host-Based Protection)

This topology is ideal for Ignition Gateways running on standard operating systems like Windows or Linux, or in cloud environments (AWS/Azure).

- **Component:** The BlastShield Agent software is installed directly on the OS hosting the Ignition Gateway.
- **Mechanism:** The Agent creates a virtual network interface (e.g., blast0) with an overlay IP address (typically in the 100.64.x.x range).
- **Configuration Steps:**
  1. Install BlastShield Agent on the Ignition Server.
  2. Configure Ignition to bind its web server and Gateway Network services to the BlastShield virtual interface IP, or simply rely on the overlay routing.
  3. Configure the host firewall (Windows Firewall or iptables) to block all inbound traffic on ports 8088, 8043, and 8060 on the physical interface (Ethernet/Wi-Fi).
  4. **Result:** The server is now deaf to the outside world. It will only accept traffic coming through the secure BlastShield tunnel.

The Gateway Model (Edge/Brownfield Protection)

This topology is used for devices where software cannot be installed, such as proprietary PLCs, legacy HMIs, or closed Ignition Edge appliances.

- **Component:** The BlastShield Gateway (available as x86 hardware, virtual machine, or container) acts as a bridge.
- **Mechanism:** The Ignition device connects to the LAN side of the BlastShield Gateway. The BlastShield Gateway connects to the WAN.
- **Configuration Steps:**

1. Place the BlastShield Gateway in front of the Ignition device.
   2. The BlastShield Gateway establishes the secure tunnel to the mesh.
   3. Remote users connect to the BlastShield Gateway, which proxies the traffic to the Ignition device behind it.
   4. **Result:** The legacy device is "cloaked" by the Gateway. It effectively receives a Zero Trust retrofit without firmware upgrades.

Securing the Gateway Network

The Gateway Network is the backbone of Enterprise Ignition architectures. Securing it with BlastShield creates a "Virtual Dark Fiber" network.

- **Scenario:** A Headquarters Gateway needs to sync with 50 Remote Site Gateways.
- **Integration:**
  1. BlastShield Agents are installed on the HQ Server and all Remote Servers.
  2. A policy is defined in the BlastShield Orchestrator: Allow Group 'Remote_Gateways' to connect to 'HQ_Gateway' on TCP/8060.
  3. Synchronization traffic flows over the BlastShield peer-to-peer, encrypted tunnel.
  4. **Benefit:** The "Hub" gateway at HQ does not need any open ports on the corporate firewall. The connection is outbound-initiated by the agents to the broker, then established peer-to-peer. This eliminates the need for complex DMZ configurations or exposing the critical synchronization port to the internet.

Securing Mobile Access (Perspective Module)

Ignition Perspective allows for mobile-first SCADA. BlastShield secures this mobile workforce.

- **Workflow:**
  1. **Authentication:** The plant manager opens the BlastShield Mobile Authenticator app. They authenticate via FaceID.
  2. **Connection:** The app establishes a transparent tunnel to the Ignition Gateway.
  3. **Application Access:** The manager switches to the Ignition Perspective app or a mobile browser. They navigate to the Ignition project URL (e.g., https://100.64.0.5:8043).
4. **Access Granted:** The page loads instantly.
- **Security Assurance:** If the phone is stolen, the thief cannot pass the biometric check. If the URL is shared, it is unreachable from any device not on the BlastShield network.

Operational Value and Total Cost of Ownership (TCO)

Beyond the security imperatives, the combined Ignition and BlastShield solution drives significant operational efficiencies, directly impacting the bottom line.

Infrastructure Cost Reduction

Traditional remote access requires static IP addresses and complex firewall hardware at every remote site.

- **NAT Traversal:** BlastShield works seamlessly behind Network Address Translation (NAT). This allows remote sites (e.g., pump stations) to use low-cost, dynamic IP cellular plans (LTE/5G) instead of expensive static IP APNs or MPLS lines.
- **Hardware Consolidation:** By using the software-based Agent, organizations can eliminate the need for dedicated VPN concentrator hardware or edge firewalls in cloud deployments.

Reduced Operational Expenditure (OpEx)

The hidden cost of network security is labor. Managing firewall rules for hundreds of sites is a full-time job for a team of engineers.

- **Policy Orchestration:** BlastShield utilizes a cloud-based Orchestrator. An administrator can grant or revoke access to a specific user or device in seconds from a central dashboard.
- **Simplified Commissioning:** Deploying a new remote site is as simple as shipping a preconfigured gateway or installing an agent. The device automatically calls home, authenticates, and receives its security policy. There is no need to configure local firewall rules or troubleshoot IPsec tunnels.

Performance and Latency

In industrial automation, latency is not just an annoyance; it is a technical constraint.
High latency can cause SCADA timeouts and data gaps.

Table 1: Performance Comparison

Feature	Traditional VPN	BlastShield (SDP)
Architecture	Hub-and-Spoke (Hairpinning)	Peer-to-Peer Full Mesh
Throughput	Limited by Concentrator CPU	**Up to 34x Faster**
Latency	High (Traffic detours to HQ)	Low (Direct path)
Connection Time	Slow (Handshakes, multiple hops)	Instant (Always-on capability)

Regulatory Compliance

The solution directly supports compliance with key industrial standards:

- **IEC 62443:** The microsegmentation capabilities allow organizations to define “Zones” and “Conduits” logically, enforcing the principle of least privilege required by the standard.
- **NIS2 Directive:** For European operators, the requirement to secure supply chains and remote access is mandated. BlastShield’s biometric MFA and encryption meet the directive’s strict access control requirements.

Sector-Specific Use Cases

The versatility of the combined solution allows it to address unique challenges across various industrial verticals.

Water and Wastewater: The Distributed Challenge

Water utilities operate highly distributed networks of lift stations, reservoirs, and treatment plants, often in remote locations.

- **The Challenge:** Connecting hundreds of remote telemetry units (RTUs) via cellular networks exposes them to the public internet. "Hackers for Water" scenarios have demonstrated the risk of unauthorized access to chemical dosing systems.16
- **The Solution:** Deploying BlastShield on Ignition Edge devices at each lift station.
- **Impact:** The lift stations become invisible. Even if the cellular IP is scanned, the device does not respond. Maintenance crews can access the station securely from their trucks using tablets with biometric authentication, eliminating the need for shared keys or static passwords.

Oil and Gas: Protecting the Upstream and Midstream

The Oil & Gas sector faces a "perfect storm" of aging infrastructure and sophisticated threats.

- **The Challenge:** Protecting legacy PLCs and SCADA systems on drilling rigs or pipeline valves running on obsolete protocols (Modbus) that cannot be patched. Reconnaissance targeting Modbus/TCP port 502 increased by 2000% in 2022.
- **The Solution:** Network Cloaking. By placing these assets behind a BlastShield Gateway, the vulnerable Modbus ports are hidden from the network.
- **Impact:** The risk of "unpatchable" vulnerabilities is mitigated. The asset remains operational but is accessible only to authenticated personnel. This significantly lowers the TCO compared to the alternative: a "rip and replace" of the legacy hardware.

Manufacturing: Secure Vendor Access

Modern factories rely on Original Equipment Manufacturers (OEMs) to remotely troubleshoot complex machinery.

- **The Challenge:** Giving a vendor VPN access to the plant network is risky. They often receive broader access than necessary, violating the principle of least privilege.
- **The Solution:** Microsegmentation. The plant administrator creates a BlastShield policy that grants the vendor access only to the specific IP address and port of the machine they support.
- **Impact:** The vendor enters a "micro-tunnel." They cannot scan the network, access the MES system, or see other machines. The "blast radius" of a compromised vendor credential is effectively reduced to zero.

Conclusion

The industrial landscape is evolving at a pace that legacy security models cannot keep pace with. The convergence of IT and OT, driven by platforms like Ignition, has unlocked unprecedented operational value but also exposed the fragility of the "air gap" and the inadequacy of perimeter defenses. The integration of BlastWave's BlastShield with Inductive Automation's Ignition offers a definitive answer to this challenge.

By overlaying a passwordless, biometric-secured, and invisible software-defined perimeter on top of the Ignition architecture, organizations can achieve the holy grail of industrial security: Zero Trust Network Access. This solution does not merely "harden" the perimeter; it renders the target invisible.

For the C-suite, the value proposition is clear: a dramatic reduction in cyber risk, a lower Total Cost of Ownership through simplified operations, and the agility to deploy remote connectivity without fear. For the engineer, it means faster, always-on access to the data they need, without the friction of legacy VPNs.

As industries from water treatment to energy production face an increasingly hostile digital environment, the partnership between Inductive Automation and BlastWave provides a robust, scalable, and proven blueprint for the future of secure industrial automation. The "Invisible SCADA" system is no longer a theoretical concept; it is a deployed reality, safeguarding the critical infrastructure that powers our world.

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

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