WHITE PAPER

Zero Trust Shielding for Manufacturing Networks

Achieving Operational Resilience and Cost-Efficiency with BlastWave's Zero Trust OT Security

BlastWave

TLDR

The accelerating convergence of Information Technology (IT) and Operational Technology (OT) systems in manufacturing, a hallmark of Industry 4.0, has significantly expanded the attack surface, rendering traditional security measures ineffective. Cyber incidents impacting these converged environments are increasingly commonplace, prompting a shift in how manufacturing organizations approach cybersecurity.

The expanding risk landscape necessitates a Zero Trust security paradigm. The "Never trust, always verify" principle is no longer theoretical, but an operational imperative, particularly for the vulnerable OT systems that underpin manufacturing processes.

Adopting a Zero Trust model in OT is not merely an aftermarket controls upgrade; it represents a strategic pivot essential for maintaining business continuity and resilience in an era of advanced, often AI-powered, cyber threats. OT security models, which historically relied on perimeter defenses, are failing to protect against attackers who can bypass these perimeters or originate from within the organization.

BlastWave is a Zero Trust solution designed for the challenges of manufacturing environments. It provides a triad of protective capabilities: network cloaking, passwordless secure remote access (SRA), and software-defined microsegmentation that collectively block entire classes of cyber risk. For Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs), BlastShield delivers tangible benefits: Zero Trust security enhancements designed to maintain uptime and safety, with significantly lower deployment times and operational costs. BlastWave provides a cost-effective and pragmatic way for manufacturers to align with IEC standards.

BlastWave's solutions:

- Deploy in hours, not years
- Do not require downtime or network architecture changes (like IP address changes for OT devices)
- Require half the maintenance effort of firewalls
- Costs ¼ the TCO of NGFW solutions

By implementing BlastWave's robust Zero Trust model, manufacturing organizations can transform their cybersecurity posture from a reactive cost center into a proactive enabler of operational excellence and a source of competitive advantage.

BlastWave

CONTENTS

The Unseen Battlefield:
Critical OT Cybersecurity Needs in Modern Manufacturing

Industry 4.0, characterized by the adoption of Connected Workers, Lights-Out Factories, and Remote Operations/Augmented Workforce tools (AR/VR), is undergoing rapid transformation, bringing efficiency and operational benefits, but also an expanded attack surface.

The Convergence Challenge:
Increased Connectivity and Expanded Attack Surfaces in Industry 4.0

Industry 4.0 is characterized by the deep integration of Operational Technology (OT) systems, such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and Manufacturing Execution Systems (MES), into enterprise-level systems and data lakes. While beneficial for productivity, this convergence renders the traditional "air gap" that once isolated OT environments, ineffective.

Approximately 50% of OT systems currently connect directly to corporate IT networks, with this number expected to rise to 70% within the next few years. Increased connectivity means that IT vulnerabilities and attacks can spread more readily into OT networks. In the past year, 75% of cyber incidents affecting manufacturing firms occurred in operations with converged IT-OT networks. This increased IT-OT connectivity makes seemingly less critical systems, like an HVAC contractor's remote access point, a gateway for attackers to reach and compromise operationally critical manufacturing systems. Perimeter defenses alone cannot mitigate threats associated with Industry 4.0.

Stopping These Attacks:
Prevent Hackers from discovering your network and having no credentials to be stolen

Key Threat Vectors:
Ransomware, Supply Chain Vulnerabilities, Insider Risks, and Legacy System Exploits

Manufacturing OT environments are targeted by a diverse range of threat vectors, each capable of causing significant disruption:

Ransomware has become the most frequent and damaging type of cyberattack against the manufacturing sector. As many as 65% of manufacturing companies have faced a ransomware attack, with the manufacturing industry being the primary target for such extortion attempts. The financial impact is staggering, with average ransom payments substantial and downtime costs accumulating rapidly, sometimes at a rate of millions of dollars per day.

- A notable example is the Norsk Hydro attack in 2019, where LockerGoga ransomware infected the company's IT systems, resulting in widespread operational disruptions across its global manufacturing plants. The attack affected 22,000 computers in 170 locations across 40 countries, forcing the company to revert to manual operations in many areas and incurring costs between $40 million and $70 million.
- More recently, the Clorox cyberattack in August 2023 led to unauthorized activity on IT systems, resulting in significant disruptions to business operations, reduced production rates, and impacted product availability. The company reported that the incident resulted in a cost of $356 million.

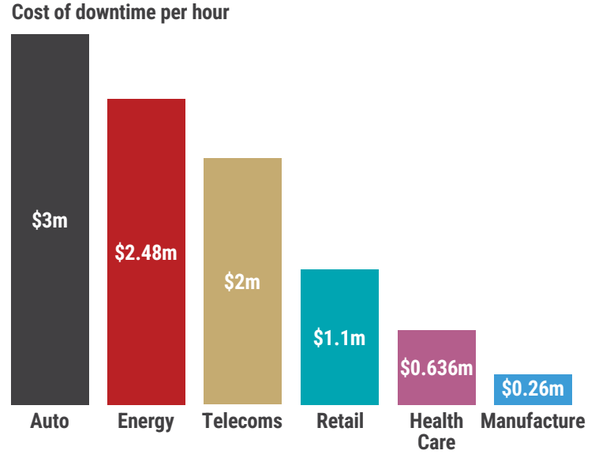
Supply Chain Attacks: Attackers increasingly target manufacturers through their less secure suppliers or third-party vendors. A compromised supplier can inadvertently introduce malware or provide an entry point into the manufacturer's network. As many as 40% of cyberattacks are estimated to occur via the supply chain. The widely publicized Colonial Pipeline attack, which disrupted fuel supplies in the US, was initiated through a compromised VPN account belonging to a third party, illustrating the potential cascading effects of supply chain vulnerabilities.

Insider Risks: Human factors, whether malicious intent or negligence, remain a significant vulnerability. Employees or contractors with legitimate access can inadvertently or deliberately cause harm. The 2021 Oldsmar water treatment plant incident, where an attacker attempted to poison the water supply, is believed to have involved the exploitation of legitimate remote access credentials, potentially by an insider or someone who had acquired insider credentials.

Legacy System Exploits: Many manufacturing facilities rely on legacy OT systems and components that were designed and deployed decades ago, long before cybersecurity became a significant concern. These systems often run outdated software, lack modern security features, and may no longer receive security patches from vendors, making them vulnerable to exploitation. The persistence of these unpatchable vulnerabilities creates a critical challenge, necessitating security solutions that can protect these systems externally through network cloaking and segmentation, as traditional endpoint security is often not feasible.

Other Pervasive Threats: Beyond these, manufacturers also face threats from sophisticated phishing campaigns (often enhanced by AI), direct attacks on Internet of Things (IoT) and Operational Technology (OT) devices, Distributed Denial-of-Service (DDoS) attacks, cloud security breaches, and the exploitation of zero-day vulnerabilities. Spear phishing and exploiting public-facing applications create infection vectors in many manufacturing breaches.

The financial motivation behind most of these attacks (96% of attacks targeting the manufacturing sector driven by monetary gain) indicates that adversaries are increasingly sophisticated in identifying and exploiting OT systems that can cause maximum operational disruption. This capability increases the pressure on victims to pay ransoms or allows for effective industrial espionage, making proactive and robust defense mechanisms more critical than ever.



The Real Costs of an OT Breach:
Beyond Financial Loss to Reputational Damage and Operational Paralysis

The consequences of a successful cyberattack on a manufacturing OT environment extend far beyond immediate financial losses. While the direct costs of downtime can be enormous, ranging from $200,000 to $2 million per incident for resilience or availability issues, and averaging $1.9 million per day of downtime in ransomware cases, the indirect and long-term impacts can be even more devastating.

Cyberattacks can cause permanent damage to expensive plant machinery and equipment, as seen in the 2014 attack on a German Steel Mill. In this incident, attackers used spear-phishing emails to steal credentials, gained access to the office network, and then pivoted to the production systems. They compromised PLCs controlling a blast furnace, preventing its proper shutdown and causing "massive" physical damage, with repair costs estimated in the millions of dollars.

Beyond physical damage, breaches can result in an inability to fulfill customer orders, significant loss of brand value, and lasting reputational harm. The operational paralysis from a major OT incident can take weeks or even months to fully resolve, impacting supply chains, customer relationships, and market confidence.

BlastWave's Zero Trust Protection:
Revolutionizing Manufacturing OT Cybersecurity

BlastWave's BlastShield solution embodies this paradigm shift, offering a comprehensive Zero-Trust protection platform specifically designed to address the unique challenges of OT.

The Zero Trust Mandate for OT:
"Never Trust, Always Verify"

The core tenet of Zero Trust is simple yet powerful: "Never trust, always verify." This means that no user, device, or application is implicitly trusted, regardless of whether it is inside or outside the traditional network perimeter. Every access request must be authenticated and authorized before access is granted, and access is limited to only the resources strictly necessary for the task at hand (least privilege).

This approach is particularly critical for OT environments because it assumes that breaches are not only possible but potentially have already occurred, and that attackers may already be present within the network. Traditional perimeter defenses are often insufficient to stop attackers who have gained an initial foothold. BlastWave's Zero Trust approach is designed to eliminate entire classes of common attack vectors like reconnaissance and phishing, fundamentally altering the security landscape for OT administrators.

BlastWave's Triad of Protection (BlastShield)

BlastShield™ delivers its Zero Trust capabilities through an integrated triad of core technologies: Network Cloaking, Passwordless Secure Remote Access (SRA), and Software-Defined Microsegmentation.

Network Cloaking:
This innovative feature renders OT networks and their constituent devices – including PLCs, SCADA systems, HMIs, and RTUs – invisible to unauthorized discovery attempts, both from external attackers and from compromised systems within the IT network. The principle is straightforward: "What you can't see, you can't attack".

By effectively blocking the reconnaissance and discovery phases of the cyber kill chain, network cloaking prevents attackers, including those leveraging AI-enhanced reconnaissance tools, from identifying potential targets and their vulnerabilities.

This proactive prevention mechanism fundamentally alters the attack lifecycle. Instead of merely making attacks harder, it makes many attack paths entirely non-viable from the outset, significantly reducing the overall threat landscape that CISOs must manage.

How Network Cloaking Works
Network Cloaking weaponizes Network Address Translation (NAT) by hiding the internal address of each device behind the BlastShield behind a "secure overlay" network, where the only connections allowed to the addresses are Zero Trust authenticated users with the proper least privilege access permissions. Cloaking requires no network reconfiguration or IP address changes, further simplifying deployment in environments where overlapping addresses can become a problem across multiple sites or networks.

Passwordless Secure Remote Access (SRA):
BlastShield™ provides robust and secure remote access for all users, including employees, third-party vendors, and maintenance contractors, without relying on vulnerable passwords. It employs phishing-resistant, biometric-based multi-factor authentication (MFA) for every access attempt. This is crucial because as high as an estimated 95% of successful hacks begin with a compromised credential, often obtained through phishing.

BlastWave's passwordless MFA is designed to protect against sophisticated GenAI-powered phishing attacks and MFA hijacking techniques. Secure, end-to-end encrypted peer-to-peer tunnels are established for all remote traffic, safeguarding data in transit. This capability directly blocks the initial access attack vector, addressing a significant vulnerability, especially in the context of widespread remote work and third-party system interactions, and overcomes the inherent weaknesses of traditional VPNs.

How Passwordless SRA Works
Passwordless MFa works the same way that Apple Pay and Google Wallet work on your mobile device. When you scan the BlastShield QR code during authentication, it validates that you are using the authorized device and that the mobile device validates your biometrics. Only then is the user allowed to select which network they will access with the BlastShield Client. There are no credentials to steal, and no phishing is possible.

Software-Defined Microsegmentation:
BlastShield simplifies the creation of granular network segments by establishing simple, peer-to-peer, encrypted, and authenticated tunnels to each device or logical group of devices (zones). This is achieved through software-defined policies, eliminating the need for complex and often error-prone firewall rulesets. This approach rigorously enforces the principle of least privilege, ensuring that users and devices have access only to the specific resources for which they are authorized. Crucially, it prevents lateral movement within the network; if one segment or device is compromised, the breach is contained, and attackers cannot easily move to other parts of the OT environment.

BlastShield can even provide lateral movement protection at Layer 2 for local network connections. This directly blocks the lateral movement attack vector, a common tactic attackers use to escalate privileges and reach high-value targets after an initial compromise.

How Software Defined Microsgementation Works
The Layer 2 switch to which the BlastShield gateway is connected is set to port isolation mode, which forces all traffic, including traffic on a flat Layer 2 network, through the gateway for policy evaluation. Users with access to the Layer 2 network cannot bypass the gateway as they would a traditional firewall; instead, the gateway determines whether each flow is permitted to pass based on the active policies.

The combination of passwordless SRA and microsegmentation creates a robust defense-in-depth for access control. Even if a novel attack hypothetically bypassed the strong authentication layer, microsegmentation would still severely limit the "blast radius," curtailing an attacker's ability to cause widespread damage.

The integrated nature of BlastWave's triad – cloaking, passwordless SRA, and microsegmentation – offers a more holistic and potentially simpler path to Zero Trust for OT than attempting to assemble and manage multiple disparate point solutions from different vendors. Such multi-vendor approaches often lead to integration challenges, policy inconsistencies, increased complexity, and a higher total cost of ownership (TCO).

Alignment with NIST Cybersecurity Framework (CSF) and Zero Trust Architecture (NIST SP 800-207)

BlastShield supports manufacturing security programs aligned with key industry standards and frameworks, notably the NIST Cybersecurity Framework (CSF) and NIST Special Publication 800-207, "Zero Trust Architecture." This alignment ensures that manufacturing organizations can trust the solution to adhere to widely recognized best practices.

BlastWave's architecture is fundamentally built on the principles outlined in NIST SP 800-207, which guides migrating to a Zero Trust architecture and the NIST Cybersecurity Framework 2.0. This includes enforcing granular access control, securing all communications, and gaining visibility into network activity, although BlastWave focuses on preventing unauthorized visibility.

Table 1: Mapping Manufacturing OT Risks to BlastWave's Zero Trust Capabilities

Common Manufacturing OT Risk	BlastWave Protective Feature(s)	How BlastWave Mitigates
Ransomware via Phishing/Credential Theft	Passwordless SRA, Network Cloaking	Eliminates passwords, uses phishing-resistant biometric MFA to prevent initial credential compromise. Cloaking makes potential targets invisible, reducing the attack surface for ransomware deployment.
Lateral Movement from IT to OT Network	Software-Defined Microsegmentation, Network Cloaking	Isolates OT segments from IT, preventing unauthorized east-west traffic flow. Cloaking OT assets makes them undiscoverable from a compromised IT segment.
Third-Party/Vendor Compromise	Passwordless SRA, Software-Defined Microsegmentation	Provides secure, passwordless access for vendors with granular, least-privilege controls via microsegmentation, limiting access to only necessary systems. Permissions can be granted/revoked in real-time.
Exploitation of Legacy/Unpatched OT Devices	Network Cloaking, Software-Defined Microsegmentation	Cloaks vulnerable legacy devices, making them invisible to attackers. Microsegmentation isolates these devices, restricting communication to only essential, authorized paths, acting as a "virtual patch".
Insider Threats (Malicious or Negligent)	Software-Defined Microsegmentation, Passwordless SRA	Microsegmentation enforces least privilege, limiting what an authenticated internal user can access or damage. Strong authentication for all access, including internal, reduces risk from compromised internal accounts.
Reconnaissance and Discovery by Attackers	Network Cloaking	Makes the entire protected OT network and its devices invisible to network scans and probes, preventing attackers from identifying targets or mapping the network architecture.
Man-in-the-Middle (MitM) Attacks	Passwordless SRA (Encrypted Tunnels)	Establishes secure, end-to-end encrypted peer-to-peer tunnels for all authenticated communications, protecting data in transit from interception or modification.
Exploitation of VPN Vulnerabilities	Passwordless SRA	Replaces traditional VPNs with a more secure, Zero Trust-based remote access solution that does not rely on passwords and incorporates stronger, phishing-resistant authentication, eliminating VPN-specific vulnerabilities.

Delivering on the Promise:
BlastWave's Superior Approach to IEC 62443 and Risk Reduction

Achieving compliance with the IEC 62443 standard, particularly its requirement for network segmentation via zones and conduits, is a crucial goal for manufacturing organizations seeking to enhance their operational technology (OT) security. BlastWave provides a means to quickly (within hours) integrate OT networks with minimal downtime (seconds), whereas traditional segmentation cannot. BlastWave deployments have reduced security-related maintenance by half, and additional methods, especially in terms of effectiveness, manageability, and overall risk reduction, offer advantages over a firewall-centric architecture.

Software-Defined Segmentation:
A Leap Beyond Traditional Firewalls for IEC 62443 Zones & Conduits

Traditional approaches to implementing IEC 62443 zones and conduits have heavily relied on physical hardware firewalls to enforce segmentation. Real-world implementations are characterized by operational complexity, significant security-related labor demands, and the potential to introduce risk into manufacturing processes. BlastWave's software-defined segmentation (SDS) provides an innovative and more flexible approach to realizing the vision of IEC 62443.

Superior Implementation of Zones and Conduits: With BlastShield, zones are created as logical groupings of devices based on similar functionality or security requirements. Communication between these zones (the conduits) is then regulated by dynamic, software-based policies rather than static, hardware-bound firewall rules.

This software-centric approach significantly reduces the complexity inherent in managing multiple physical firewalls and their often convoluted rule sets, which customers frequently struggle with, sometimes resorting to insecure "any/any" rules just to maintain connectivity. BlastWave's method requires no network reconfiguration or IP address changes, further simplifying deployment.

Enhanced Effectiveness and Risk Reduction: BlastWave's SDS provides enhanced security by effectively isolating zones and limiting the spread of potential attacks. It allows for highly granular control, enabling security teams to tailor access rules for specific devices, users, and communication protocols, including remote access for service providers.

This is particularly valuable for isolating vulnerable legacy devices, such as older PLCs, restricting their communication to only essential and authorized systems. BlastWave's segmentation can act as a "virtual patch" for these unpatchable systems, blocking exploit-prone protocols and isolating inherent risks without requiring costly hardware replacement or disruptive system downtime.6 This "virtual patch" capability is a critical enabler for extending the secure operational life of expensive OT equipment, allowing organizations to defer costly upgrades while effectively mitigating associated risks.

Simplified Deployment, Management, and Adaptability: Managing hardware firewalls can be cumbersome, error-prone, and often requires operational downtime for updates or changes – a significant challenge in 24/7 manufacturing environments. BlastWave's SDS overcomes these limitations. It enables more straightforward configuration and maintenance, even for teams with limited dedicated cybersecurity expertise. Policies can be updated in real-time to address evolving threats or changing operational needs without disrupting production.

This agility and ease of management make it achievable for a broader range of manufacturing organizations to achieve robust IEC 62443 alignment, including those with constrained budgets or smaller security teams that might find traditional firewall-heavy architectures prohibitively complex and expensive..

"We haven't segmented our network because it will take us two years and too much downtime with our current firewall vendor"

ANONYMOUS CUSTOMER

Table 2: IEC 62443 Zone & Conduit Implementation: BlastWave SDS vs. Traditional Firewalls

Aspect	Traditional Hardware Firewalls	BlastWave Software-Defined Segmentation (SDS) with BlastShield™
Granularity of Control	Typically, zone-to-zone, device-specific rules are complex and often limited by the capabilities of firewalls.	Highly granular; user, device, application, and protocol-specific policies for precise control.
Ease of Management & Deployment	Complex configuration, multiple devices to manage, potential for rule conflicts, and often required network changes.	Simplified, centralized policy management via software; no network reconfiguration or IP changes needed.
Adaptability to Change	Slow to adapt; changes often require manual reconfiguration of multiple firewalls and potential downtime.	Policies can be highly adaptable in real-time without downtime to respond to new threats or operational needs.
Cost (CapEx/OpEx)	High CapEx for hardware; significant OpEx for management, maintenance, and specialized personnel.	Lower CapEx (reduced hardware need); significantly lower OpEx due to simplified management and automation.
Risk Reduction Effectiveness	Can be effective if perfectly configured, but complexity leads to a risk of misconfiguration; lateral movement is still possible if the rules are too permissive.	More effective at preventing lateral movement due to granular, identity-based policies; reduces misconfiguration risk.
Complexity	High; managing numerous rulesets across distributed firewalls is a significant challenge.	Low; intuitive software-based policy creation and management.
Downtime for Changes	Often requires scheduled downtime for significant policy changes or hardware upgrades.	Minimal to no downtime for policy changes; software updates can often be applied non-disruptively.

Passwordless SRA for Third-Party Access:
Secure, Auditable, and Efficient

Managing remote access for third-party vendors and maintenance contractors is a notorious challenge in OT security. These external entities require legitimate access to OT systems for support, updates, and troubleshooting, but their access also introduces significant risk if not properly controlled. The infamous Target data breach, which originated through the compromised credentials of an HVAC contractor, serves as a stark reminder of this vulnerability.

BlastWave's passwordless Secure Remote Access (SRA) directly addresses this critical pain point:

- **Eliminating Credential-Based Risk:** By employing phishing-resistant, biometric-based multi-factor authentication (MFA), BlastShield reduces the reliance on passwords for third-party access, thereby mitigating the risk of exploiting stolen or weak credentials.
- **Granular, Least-Privilege Access:** BlastWave enables the real-time granting and revocation of access permissions for contractors and part-time staff, ensuring they can only access the specific OT systems and perform the specific functions necessary for their tasks. This is enforced through microsegmentation, preventing any lateral movement from their designated access points.
- **Enhanced Auditability and Control:** All access sessions are authenticated and can be logged, providing a clear audit trail for compliance and security monitoring purposes.

This combination of passwordless SRA and microsegmentation for third parties not only secures access but also fundamentally changes the trust model for external collaborators. It enables manufacturing organizations to engage with vendors more agilely and efficiently, facilitating faster issue resolution and improved support, without incurring the traditional trade-offs between operational necessity and security integrity.

Achieving Operational Excellence and Reduced Costs with BlastWave

For manufacturing CISOs and CIOs, cybersecurity investments must mitigate risk, support core business objectives, and demonstrate a clear return on investment. BlastWave's BlastShield™ solution is engineered to deliver on both fronts, enabling operational excellence while significantly reducing the total cost of ownership (TCO) for OT security.

Maximizing Uptime and Ensuring Production Continuity

One of the most critical operational goals in manufacturing is maximizing uptime. Unplanned downtime due to cyberattacks can lead to millions of dollars in lost production, missed deadlines, and contractual penalties. BlastWave's proactive prevention capabilities are designed to minimize this risk. By blocking initial access, preventing reconnaissance, and stopping lateral movement, BlastShield helps ensure that production lines continue to run smoothly.

A compelling real-world example underscores this benefit: BlastWave's Zero Trust Protection kept a manufacturing plant operational during a cyberattack that could have otherwise resulted in an estimated $4.8 million in losses over a two-day period.

In this incident, BlastWave's solution successfully blocked the attackers from gaining initial access to the protected OT segment, cloaked the critical OT systems, making them undiscoverable, and prevented any lateral movement from other compromised parts of the network, thereby isolating and neutralizing the threat before it could impact production.

Protecting Critical Assets and Intellectual Property

Manufacturing OT environments house critical assets, including PLCs, SCADA systems, MES, robots, and industrial IoT devices, which control physical processes.10 Unauthorized access to or manipulation of these systems can lead to equipment damage, safety incidents, or compromised product quality.

BlastWave safeguards these vital assets by ensuring only authenticated and authorized users and processes can interact with them. Furthermore, manufacturers possess valuable intellectual property, including designs, formulas, and proprietary methods, which are prime targets for industrial espionage. BlastWave's robust access controls and data protection mechanisms help prevent the exfiltration of sensitive information, thereby preserving its competitive advantage.

Reduced Total Cost of Ownership (TCO) for OT Security

BlastShield offers a significantly lower total cost of ownership (TCO) than traditional, often hardware-centric, OT security approaches.7 This is achieved through several key factors:

Lower Capital Expenditure (CapEx): The software-defined nature of BlastShield™, particularly its microsegmentation capabilities, significantly reduces the need for extensive investments in numerous hardware firewalls and other physical security appliances. BlastShield's simplicity directly translates to lower upfront costs.

Streamlined Deployment Processes: Traditional security solutions can be complex and time-consuming to deploy, often requiring significant network reconfiguration and downtime. BlastShield is designed for rapid deployment, reportedly installing in as little as one-tenth the time needed for traditional solutions. It can be implemented without a major IT overhaul or significant changes to the existing network architecture, often working in tandem with existing infrastructure.

Notably, BlastWave's software-defined microsegmentation eliminates the need for network reconfiguration or IP address changes, significantly simplifying the deployment process. This rapid and less disruptive deployment enables security teams to achieve a higher level of OT protection more quickly.

Simplified Operational Management (OpEx): The ongoing management of traditional security infrastructure, particularly complex firewall rulesets, can be a significant operational burden, requiring specialized skills and a substantial time investment. BlastShield™ offers approximately half the management overhead compared to traditional IT-centric security solutions. Its centralized, software-based policy management simplifies configuration and maintenance, making it easier for existing teams to manage effectively, even those with limited dedicated cybersecurity staff.

The reduction in complexity of firewall rulesets further contributes to lower OpEx. The efficiency gains free up skilled security personnel to focus on other strategic initiatives rather than being consumed by intricate security configurations.

BlastWave's solution can protect networks at approximately one-quarter of the cost associated with traditional solutions, factoring in these CapEx and OpEx advantages and BlastWave's lower acquisition costs.

Table 3: BlastShield Benefits

Benefit Type	Benefit Description	Benefit Detail	Estimated Benefit Basis	Economic Benefit (Low)	Economic Benefit (High)
Time Savings	Rapid deployment and simplify divestiture during M&A	Deployment via BlastShield within 3 weeks post-acquisition with limited truck rolls	2–4 weeks saved per acquisition; 1–2 weeks saved per divestiture	**$208,000**	**$416,000**
Time Savings	Real-time access control	Instant zero trust access updates	Minutes to hours saved per policy change	**$7,500**	**$7,500**
Time Savings	Pre-configure passwordless access	Immediate user access w/o password setup	1–2 hours saved per user setup	**$7,500**	**$15,000**
Tiem Savings	Eliminate password change burden on users and administrators	Eliminate user changes of passwords and admin assistance when change fails	1-2 hours saved per user per year	**$7,500**	**$15,000**
Cost Savings	Eliminate IP conflict resolution efforts	BlastShield overlay eliminates need for IP rearchitecture for overlapping addresses	$2,000–$5,000+ saved per acquisition in reconfiguration labor	**$5,000**	**$5,000**
Cost Savings	Avoid physical site visits	Automatic remote configuration eliminates need for site visit	$500–$1,500 saved per site	**$26,000**	**$78,000**
Cost Savings	Avoid overpowered IT firewalls	Replace expensive IT firewalls with cost-effective BlastShield gateways at remote sites	$5,000–$10,000 saved per site	**$100,000**	**$200,000**
Cost Savings	Simplify firewall policies	Eliminates firewall rule conflict from nested firewalls	Minutes to hours saved per policy change and troubleshooting	**$7,500**	**$7,500**
Cost Savings	Eliminate Phishing Training Costs	Eliminates costly employee phishing training and testing	$1-2 per user per user	**$5,000**	**$10,000**
Operational Resilience	Reduce Commnication Outages	Gateway link redundancy reduces connectivity outages	1 hour of lost production costs $5k per event	**$260,000**	**$780,000**
Operational Resilience	Flexible, ad hoc access for contractors and third parties	Just-in-time least privilege access for contractors	$1,000–$3,000 saved per contractor onboarding	**$530,000**	**$1,100,000**
Operational Resilience	Automation and observability enablement	Automatic device import speeds onboarding	5–10 hours saved per deployment + 20% of sites experiencing configuration errors	**$55,000**	**$60,000**
TOTAL				**$1,219,000**	**$2,694,000**

Demonstrable ROI:
The BlastWave Advantage

The return on investment (ROI) for BlastWave's solution is compelling, primarily driven by the significant cost avoidance associated with preventing cyber breaches. The $4.8 million saved by one manufacturing plant due to BlastWave preventing a major attack is a direct testament to this.

When considering the potential multi-million-dollar losses from incidents like those at Norsk Hydro ($70 million) or Clorox ($356 million), or the physical damage costs seen at the German Steel Mill, the investment in a proactive prevention solution like BlastShield becomes highly justifiable. The TCO and ROI calculations for BlastWave should heavily factor in the "cost of inaction" or the "cost of a breach," which is demonstrably very high in manufacturing OT.

This shifts the perspective from viewing security solely as an expense to recognizing it as an essential investment in risk avoidance, operational continuity, and overall business preservation. Furthermore, rapidly deploying robust security like BlastWave's can accelerate the secure adoption of new Industry 4.0 technologies and manufacturing line expansions, as security can be integrated from the outset with less friction and delay, turning a security investment into a business accelerator.

Table 4: BlastWave's Contribution to Operational Goals and Cost Reduction

Operational Goal/Cost Factor	Challenge in Traditional OT Security	How BlastWave Addresses It	Quantifiable Benefit
Maximize Uptime	Ransomware, malware, and other attacks cause significant production downtime.	Proactive prevention of breaches through cloaking, passwordless SRA, and microsegmentation limits attack vectors.	Prevented $4.8M loss in one factory by keeping lines running during an attack. Reduces the risk of costly downtime incidents.
Ensure Plant Safety	Compromised control systems can lead to unsafe operating conditions and physical damage.	Isolates critical control systems; prevents unauthorized access and manipulation that could lead to safety incidents.	Mitigates risk of physical damage and personnel injury by securing PLCs, SCADA, etc..
Protect Intellectual Property	IP theft via network intrusion is a significant concern.	Strong access controls and data flow restrictions, achieved through microsegmentation, prevent unauthorized access to sensitive data repositories.	Safeguards valuable designs, formulas, and trade secrets from exfiltration.
Reduce Security Hardware Costs (CapEx)	Heavy reliance on numerous physical firewalls and other appliances for segmentation.	Software-defined microsegmentation eliminates or significantly reduces the need for extensive hardware firewalls.	Lower upfront investment in security infrastructure.
Lower Security Admin Overhead (OpEx)	Complex firewall rule management, frequent updates, and specialized skills are required.	Simplified, centralized software-based policy management; reduced complexity; less specialized expertise needed.	"Half the management overhead" of traditional solutions. Frees up skilled personnel.
Expedite New System Deployment	Integrating security into new lines or systems can be slow and complex compared to traditional methods.	Rapid deployment capabilities; no network reconfiguration needed; security can be "baked in" with minimal friction.	"Installs in one-tenth the time". Accelerates secure adoption of Industry 4.0 technologies.
Reduce Overall Security Costs	High TCO due to hardware, complex management, and incident response costs.	Integrated solution with lower hardware needs, simplified management, and proactive breach prevention.	Protects networks at one-quarter the cost of traditional solutions, offering a significant return on investment (ROI) from breach prevention.

Conclusion:
Secure Your Manufacturing Operations with BlastWave

The manufacturing industry is navigating an era of unprecedented technological advancement, but this progress is shadowed by an increasingly sophisticated and aggressive cyber threat landscape. The operational technologies that form the backbone of modern production are prime targets, and the consequences of a breach – ranging from crippling downtime and substantial financial losses to severe safety incidents and reputational ruin – are too significant to ignore. Traditional security paradigms, rooted in perimeter defense, are no longer sufficient to protect these vital assets. A fundamental shift towards a Zero Trust security model is not just advisable; it is imperative for survival and success.

BlastWave's BlastShield™ solution offers a unique and compelling value proposition for manufacturing CISOs and CIOs striving to secure their OT environments. Through its integrated triad of network cloaking, passwordless secure remote access (SRA), and software-defined microsegmentation, BlastWave directly addresses the most critical cybersecurity needs of the sector. This approach proactively eliminates entire risk classes by making OT assets invisible to attackers, removing vulnerable passwords from the access equation, and containing any potential threats through granular segmentation that prevents lateral movement.

Crucially, BlastWave empowers manufacturing organizations to achieve their core operational objectives: maximizing uptime, ensuring plant safety, maintaining production quality, and protecting valuable intellectual property by providing a resilient and robust security foundation. The solution's strong alignment with the IEC 62443 standard, particularly its innovative and simplified approach to implementing zones and conduits, allows organizations to meet stringent compliance mandates effectively and efficiently. The significant reductions in deployment time, operational overhead, and the overall total cost of ownership further solidify BlastWave's position as a strategically sound investment. The demonstrable ROI, highlighted by instances where BlastWave has prevented multi-million dollar losses, underscores its financial viability.

For manufacturing CISOs and CIOs, BlastWave offers a clear path to simplify the inherent complexity of OT security. It provides the tools to build a security posture that is not only defensive but also adaptive and future-proof, capable of withstanding an evolving threat landscape increasingly characterized by AI-driven attacks and sophisticated adversaries targeting critical infrastructure. By adopting BlastWave, organizations are not merely purchasing a security product but investing in a strategic partnership that fosters resilient, efficient, and secure manufacturing operations, ultimately contributing to the organization's bottom line and competitive standing.

Call to Action

We invite Manufacturing CISOs and CIOs to explore how BlastWave can revolutionize their OT cybersecurity posture and help achieve strategic operational and financial goals. Take the next step towards a more secure and resilient future:

Discover the Technology:
Visit the BlastWave website at **www.blastwave.com** to download detailed technical whitepapers on BlastShield's Zero Trust capabilities and OT-specific solutions.

Assess Your Needs:
Request a personalized assessment to understand how BlastWave's network cloaking, secure remote access, and microsegmentation can address specific cybersecurity challenges within your manufacturing operations.

See it in Action: Schedule a live demonstration to witness firsthand how BlastShield™ makes OT assets invisible, provides phishing-resistant access, and prevents lateral movement within industrial networks.

Begin Your Zero Trust Journey: Protect Your Critical OT Infrastructure Quickly and Cost-Effectively. Explore options to trial BlastShield™ and experience its ease of deployment and powerful protection capabilities.

v20250619

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499