BlastWave

Zero Trust OT Cybersecurity Protection for Manufacturing

BlastWave empowers manufacturers to build impenetrable OT security by eliminating the root causes of cyberattacks, not just treating symptoms, ensuring uninterrupted production and safeguarding critical assets. We simplify robust Zero Trust protection, enabling seamless integration and operational efficiency, so you can focus on building the future of manufacturing, not defending against its threats. Manufacturing customers choose BlastWave because:

Elimination of Core Vulnerabilities: BlastWave tackles the root causes of cyberattacks, such as password vulnerabilities and network visibility, rather than just reacting to symptoms like phishing.

Protection of Legacy Systems: It provides a "virtual air gap" for unpatchable legacy devices, shielding them from modern threats without disrupting operations.

Enhanced Operational Uptime: By preventing attacks and limiting their spread, BlastWave minimizes downtime and ensures continuous production.

Simplified IEC 62443 Compliance: The solution's architecture aligns with IEC 62443 standards, simplifying compliance efforts and reducing regulatory risk.

Reduced Attack Surface: Network cloaking hides critical assets, making them invisible to attackers and drastically reducing the attack surface.

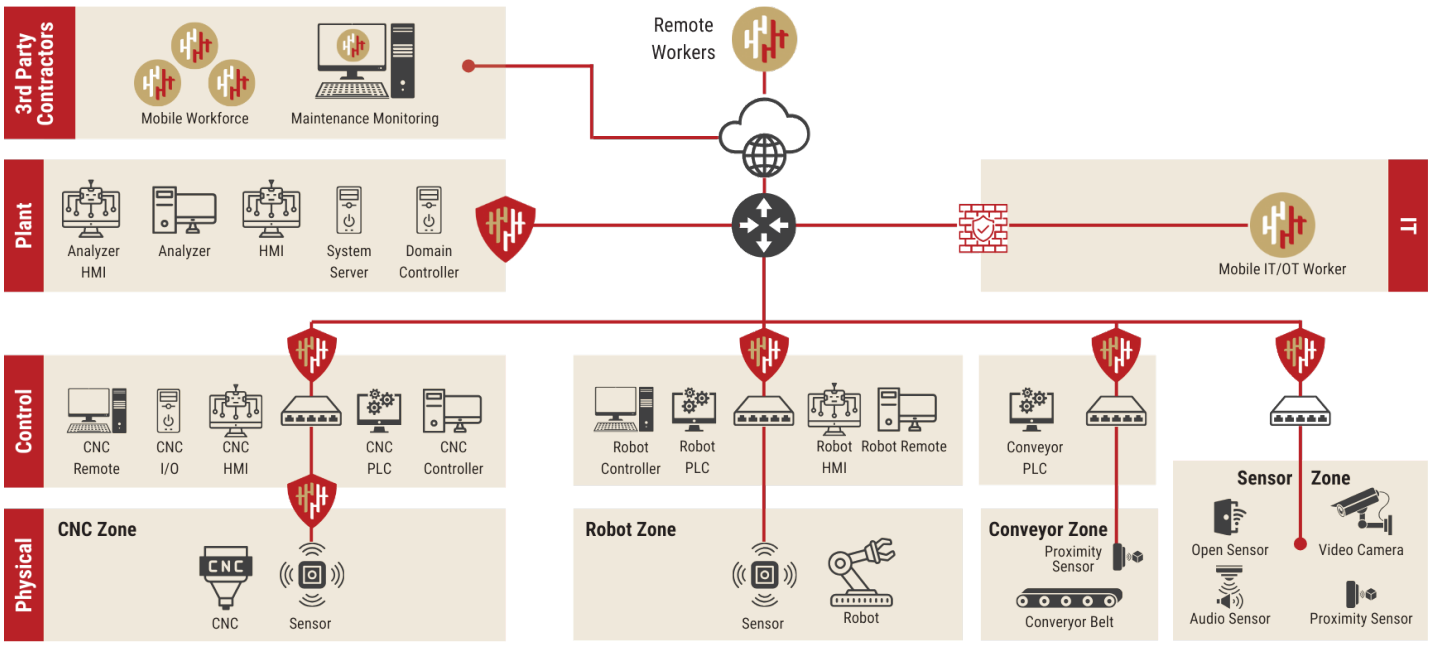
BlastShield

Mitigate Initial Attack Vector Risks with AI-resistant Reconnaissance prevention and phishing-resistant secure remote access

Ensure Cyber Resilience with software defined IEC 62443 zones and conduits to minimize risk & prevent lateral movement

Simplify Operational Complexity by deploying a solution that does not require complex hardware or a network redesign and downtime

Figure 1 Shielding Manufacturing Operations



BlastShield™: Zero Trust OT Protection for Manufacturing Systems

As the age of Industry 4.0 expands, the manufacturing industry encounters a growing threat landscape in terms of cybersecurity, with operational and information technology environments becoming more interconnected. This integration poses a big challenge since legacy solutions with significant security weaknesses are frequently involved.

Manufacturing companies do not have a consolidated set of regulations like some industries, but following the NIST Cyber Security Framework, NIS2 Directive, Cyber Resilience Act, or IEC 62443 provides strong guidance on best practices for the industry. BlastWave delivers a number of key use cases for Manufacturing:

Building IEC 62443 Zones and Conduits

With BlastWave, OT administrators can easily create secure software-defined zones and conduits that minimize risk and protect your manufacturing floor from cyberattacks. Since BlastWave's zones and conduits are software-defined, they do not require expensive and complex hardware-based firewalls to be deployed between each zone, and do not require downtime to deploy, This easy to use and easy to deploy network segmentation and microsegmentation limits the blast radius of a cyber attack and mitigates risk throughout the manufacturing network.

Securing Industrial Control Systems (ICS) and SCADA:

BlastWave Protects critical control systems from unauthorized access, preventing production disruptions, and potential sabotage. These systems can be protected from external access with a virtual air gap, enabling zero trust remote access, and east-west segmentation.

Shielding Unpatchable Legacy Equipment

Many legacy manufacturing devices can no longer be updated, and others have vulnerabilities that should not be exposed to public access. BlastWave provides a virtual air gap for legacy machines and devices that cannot be patched, safeguarding them from known and zero-day vulnerabilities. This removes the requirements for downtime and urgent patches to operational systems, increasing productivity and revenue.

Enabling Secure Remote Maintenance

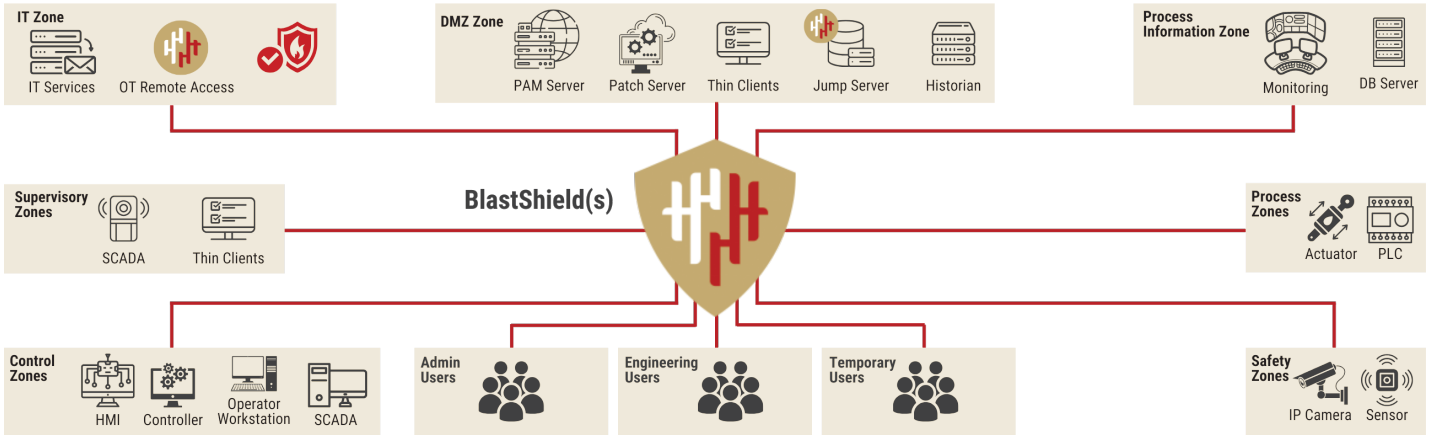
BlastWave facilitate secure remote access for maintenance personnel and third-party vendors, reducing downtime and improving efficiency. Access is limited to necessary systems and data, ensuring least privilege and mitigating risk for 3rd party access.

Ensuring Compliance with Industry Standards

Our solutions assist with compliance requirements related to cybersecurity, such as IEC 62443, NIST Cybersecurity Framework (CSF), and others. BlastWave designs in maximum protection for your OT network, delivering a secure infrastructure based on secure standards.

Zero Trust

BlastWave's Secure By Design architecture shields the OT network against AI powered reconnaissance and GenAI generated phishing. Deploying a Zero Trust architecture ensures that your network is hard to hack, yet easy to use, delivering the strongest possible security architecture without impacts your business process.



v20250403

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