OT Zero Trust Protection for the Manufacturing Industry

Software-Defined Zones and Conduits

BlastWave

The manufacturing sector is heavily targeted by cyber attacks, with AI-powered threats on the rise.

As of 2023, IBISWorld estimates that the US has over 600,000 manufacturing businesses, and SCMO estimates that there are over 10,000,000 worldwide. Manufacturing output was over $16T in 2022, making it a prime target for hackers looking to generate ransoms. IBM's X-Force Threat Intelligence Report lists Manufacturing as the top-attacked OT industry at 58% of all attacks and 25% of all industry attacks.

As manufacturing moves into the era of Industry 4.0 and beyond, the challenge of protecting their cyber-physical OT networks has become a business imperative. Cyber attacks can cause manufacturing companies to incur enormous losses in operations and revenue by forcing the closure of one or more plants while addressing the damage done. In addition, manufacturers may face exposure to sensitive data, which can result in failing to fulfill customer orders and a loss of brand value. In extreme circumstances, the most severe attacks can cause permanent damage to a manufacturer's plant and equipment. Although it brings tremendous operational advantages, the fact is that the more connected your OT environment is, the bigger the risk.

Manufacturing companies must isolate their OT networks from their IT networks and deploy a cybersecurity solution optimized for the OT environment. Software-Defined Zones and Conduits combined with Passwordless Remote Access delivers strong IEC 62443 cybersecurity protection powered by BlastWave.

CONTENTS

OT Zero Trust Protection for Manufacturing

BlastShield secures manufacturing networks, especially for IEC 62443 compliance, acting like a digital force field. It hides critical systems, segments your network into secure zones and conduits, and verifies every connection. This stops hackers from disrupting production, stealing data, and causing costly downtime, ensuring your operations run smoothly and securely. It keeps your network secure and operational, delivering a ROI that exceeds traditional cybersecurity solutions.

Key benefits of BlastWave for Manufacturing OT:

Network Cloaking for Hidden Assets:

BlastWave's network cloaking technology renders critical OT devices and systems invisible to unauthorized users and external threats. This effectively removes them from the attack surface, protecting legacy equipment and vulnerable systems that cannot be patched.

Zero Trust Segmentation and Microsegmentation

BlastWave enables granular network segmentation and microsegmentation, allowing manufacturers to create secure zones and conduits as defined by IEC 62443. This limits lateral movement, contains breaches, and protects critical assets from unauthorized access.

Passwordless Multi-Factor Authentication (MFA)

BlastWave eliminates the vulnerabilities associated with traditional passwords by implementing passwordless MFA. This ensures only authorized personnel can access the network, preventing credential theft and phishing attacks.

Secure Remote Access for Third-Party Maintenance

BlastWave facilitates secure remote access for third-party contractors and vendors, allowing them to perform maintenance tasks without compromising network security. Access is strictly controlled through passwordless MFA and segmentation, ensuring least privilege and time-limited access.

Protection Against AI-Powered Attacks

BlastWave's network cloaking and strong authentication capabilities effectively counter AI-powered reconnaissance and phishing attacks, preventing attackers from gathering information and exploiting vulnerabilities.

Simplified Compliance with IEC 62443

BlastWave's platform provides the necessary security controls to achieve and maintain compliance with IEC 62443. This simplifies the compliance process and ensures manufacturing networks meet industry best practices.

Operational Continuity & Reduced Downtime

By preventing cyberattacks and limiting the impact of breaches, BlastWave helps ensure operational continuity and minimize costly downtime. This allows manufacturers to maintain production schedules and meet customer demands.

BlastWave

BlastWave's Approach:

BlastWave implements a true Zero Trust architecture, assuming no user or device is inherently trustworthy. We verify every connection, enforce least privilege access, and continuously monitor network activity to detect and respond to threats in real-time. Our solution is designed to be easy to deploy and manage, minimizing disruption to existing operations.

By implementing BlastWave, manufacturers can strengthen their OT security posture, protect their critical assets, and ensure their facilities' continuous and secure operation in the face of evolving cyber threats.

Network Cloaking for Manufacturing

Network cloaking is like making your critical OT systems invisible to hackers. They can't attack what they can't see! This is important for protecting legacy, vulnerable equipment that can't be easily updated or can't be updated at all. It's like giving them a digital invisibility cloak, keeping them safe and your operations running smoothly.

Scenario:

A bustling manufacturing plant producing a high-value product grinds to a halt as all of its systems go offline. Cybercriminals have exploited a vulnerability in a legacy component, shutting down the production line and demanding a ransom from the manufacturer. After paying a ransom demand of over $2M, the CISO is looking for a new solution to protect them from the widespread hack that turned off their operational technology (OT) systems. Their existing firewall and VPN systems could not protect the unpatched OT systems that led to the hack, and a new approach is needed going forward. They deploy BlastShield to cloak their OT network, and their OT network can no longer be surveilled for vulnerable devices.

Industry Perspective:

The rapid digitization of the manufacturing sector, with Industry 4.0 technologies like IoT and AI at the helm, has drastically improved productivity. However, Verizon's 2022 Data Breach Investigations Report throws a spotlight on the grim reality - a majority of cyber incidents in manufacturing are driven by motives of financial gain and facilitated through tactics like social engineering, system intrusion, and web application attacks. High-profile breaches, such as those suffered by OXO International, Hanesbrands, and DuPont, underline the multifaceted threat. With the potential financial implications of an attack and 61% of manufacturing and production businesses reporting increased cyberattacks, finding the right solution for top-notch cybersecurity to provide a software-defined perimeter is paramount for manufacturing businesses.

BlastShield

Network Cloaking as a Digital Shield for Manufacturers

In a manufacturing environment, if you can't see an OT system, you can't hack or attack it. Network cloaking is the industry's best opportunity to prevent hacks. IT/OT administrators cannot patch legacy systems; zero-day vulnerabilities are even in VPN products.

BlastShield cloaks the manufacturing supply chain to make it invisible to hackers, providing a layer of defense that is impossible with firewall or VPN solutions today. BlastShield protects against inbound attacks, lateral movements, and diverse cyber threats, including stolen credentials and malware delivery, enhancing operational integrity. With BlastShield, crucial manufacturing components like workstations and building management systems remain uninterrupted and secure from outside threats.

Remote Access for Manufacturing

Secure remote access for OT is like giving authorized users a unique key to get into your critical systems from anywhere, but with extra security checks to keep out bad guys. It's important because it lets your people do their jobs without being tied to a physical location, while also protecting your essential operations from cyberattacks and costly downtime. It doesn't matter if the user is an employee, a contractor, or an emergency maintenance worker, they can only see what you want them to see, and the rest of the network is protected from unauthorized access.

Scenario:

A highly profitable manufacturing plant producing cutting-edge electronics components. The security of their SCADA system is a remote desktop application running on the server that manages the SCADA system. It has an unknown zero-day vulnerability that a hacking group has discovered but has yet to be generally known.

The IT/OT administrator only allows access to the SCADA system through the RDP application, and the system is accessible from the internet to enable the administrator to control the system from home. The hacker group discovers through reconnaissance that this system is on the IT network and exploits the newly discovered vulnerability. They alter robot control programs, leading to faulty components and production delays. While manipulating production processes, the hackers also steal proprietary data through lateral movement in the IT network. The vendor announces the vulnerability and releases a patch, but the company's secrets are splashed all over the headlines because they choose not to pay the ransom demand.

The network administrator deploys BlastWave to secure remote access to the SCADA system, and the hackers can no longer penetrate the OT network. Network cloaking prevents the SCADA system vulnerability from being discovered during the reconnaissance phase of the attack, and the biometric MFA prevents any insecure remote access.

Industry Perspective:

Manufacturing plants increasingly rely on remote access for real-time monitoring and control of production lines. Manufacturers are adopting industry-specific protocols like ISA/IEC 62443 and the NIST Cybersecurity Framework that provide best practices for securing OT systems. Despite proactive vulnerability management and network segmentation, too many legacy systems, zero-day vulnerabilities, and temporary contractor access to OT systems put manufacturing networks at risk daily.

BlastShield

Keeping Manufacturing Secure

With BlastShield, manufacturers can enable secure remote access for staff and third-party vendors, ensuring the integrity of production processes.

The solution's MFA and AES-256 encryption protect against unauthorized access, while network cloaking and microsegmenation secure the OT network infrastructure from bad actors.

Segmentation for Manufacturing

Think of network segmentation like building fences inside your factory. It separates different parts of your OT network so a problem in one area can't spread to others. Microsegmentation takes it further, putting fences around individual machines or systems. This limits the damage a hacker can do and keeps your critical operations running smoothly. Accomplishing segmentation with a software-defined solution saves time, money, and operational resources over traditional hardware-based firewall segmentation solutions.

Scenario:

A large manufacturing plant has implemented network segmentation to isolate its critical industrial control systems (ICS) from its IT network. However, the plant's ICS network has undocumented connections to its SCADA (Supervisory Control and Data Acquisition) and the IT network to enable remote access.

A hacker group gains access to the plant's IT network through a phishing email and steals sensitive data, including the login credentials for the plant's SCADA system. The attackers then use the stolen login credentials to access the plant's SCADA network, laterally move to other systems, manipulate the system to cause disruptions to plant operations and demand a ransom to release control of the systems. Rather than pay the ransom, the IT staff shut the network down and secured it using BlastShield to segment their networks and deliver Secure Remote Access.

Industry Perspective:

Network Segmentation is described by IEC 62443 within the Zones and Conduits framework. It is crucial for manufacturing companies, which operate complex and interconnected networks that span multiple locations, including factories, warehouses, and supply chain partners.

Segmentation significantly reduces the risk of cyberattacks by limiting the movement of attackers within a network, enhancing protection for Industrial Control Systems (ICS) networks. Many manufacturing industries are subject to IEC 62443 regulations that mandate network segmentation to protect critical infrastructure, and implementing network segmentation reduces risk and can help keep manufacturing lines operational even during network breaches and hacks.

According to a recent survey by the SANS Institute, 82% of manufacturing companies have implemented network segmentation or plan to do so within the next two years. By doing so, manufacturing companies can protect their critical infrastructure, prevent disruptions to operations, and comply with regulatory requirements.

BlastShield

Network Segmentation Drives Manufacturing Networks

BlastShield simplifies the challenge of microsegmentation by creating simple peer-to-peer encrypted and authenticated tunnels without complex firewall rulesets.

IT and OT network staff are permitted access only to the systems they are responsible for. BlastShield prevents lateral movement within the network with the P2P VPN connections without complex network changes, reducing the stress and workload on the limited network staff.

OT networks' flat design makes them highly vulnerable to lateral movement, complicating effective segmentation

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

v20250513

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