BlastWave

BlastShield Zero-Trust Network Access for Manufacturers

Manufacturing Is Building Back Despite Turbulence

The manufacturing industry is continuing to build back aggressively despite supply chain and labor challenges. In fact, even with the pandemic, the manufacturing industry is poised to grow 14.2% in 2022.[1] Manufacturers across multiple sectors such as electronics, automotive, discrete manufacturing, process manufacturing, industrial automation, food processing, and oil and gas are turning to digitalization, IoT, and cloud computing to improve efficiency and enable new models for growth and revenue. The hybrid workforce, supply chain instability, smart factory initiatives, and investments in environmental, social, and governance (ESG) have increased business complexity, and a new approach to cybersecurity is needed.

Managing Cybersecurity Risk

The manufacturing industry must manage cybersecurity risk to protect its supply chain and ensure the reliability of critical factory processes. A single minute of downtime can cause a major disruption that can be costly. The challenge is that digital transformation and IoT initiatives are increasing the surface of attack. At the same time, legacy systems and engineering stations running older operating systems or applications that cannot be patched, making them difficult to protect. Additionally, these older systems share the same network as many more modern systems making it difficult to standardize on endpoint security controls. Additionally, the labor shortages and need to enable a hybrid workforce of employees and contractors working remotely has put more pressure on IT and security organizations to improve antiquated remote access and VPN technologies.

BlastShield™

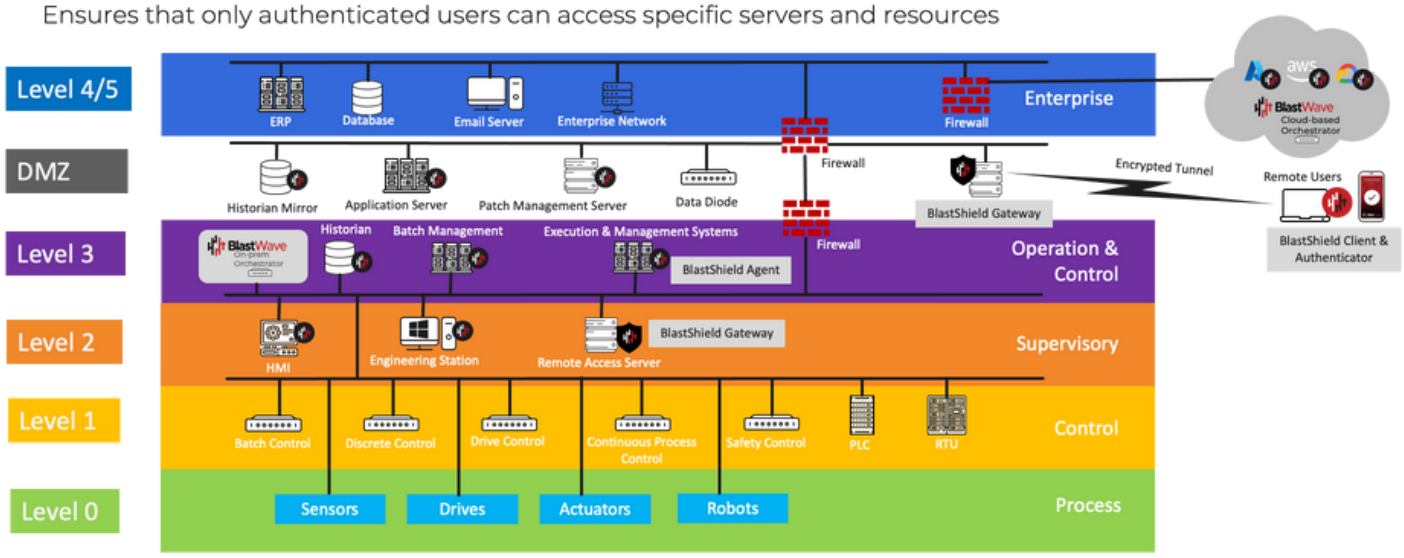
BlastShield is a zero-trust network access (ZTNA) solution that provides a more secure way to manage remote access, site-to-site access and protect against both internal and external attack vectors. By deploying BlastShield software on end user client devices and software agents on servers and gateways, OT security administrators are able to create a software-defined perimeter (SDP) that includes phishing-resistant MFA, microsegmentation, encrypted tunnels, and a security orchestration system that can operate in the cloud or in a completely air-gapped environment.

BlastShield can replace hardware-based VPNs and insecure remote access technologies. Deployed at Level 2, 3 and 3.5 (DMZ), BlastShield does not impact Control and Process systems.

[1] Manufacturing in the US - Market Size 2005–2028. IBISWorld.

BlastShield Provides Zero-Trust Network Access

Ensures that only authenticated users can access specific servers and resources



BlastShield Solution

BlastShield Authenticator

The BlastShield™ Authenticator is a downloadable software image for iOS and Android mobile devices for user password-less authentication.

BlastShield Client

The BlastShield Client provides user access into the BlastShield network. The Client is downloadable software for Microsoft Windows, macOS, iPhone iOS, and Android.

BlastShield Host and Gateway Agents

The BlastShield Host Agent is software that is easily deployed on any IP-connected physical or virtual machine running Linux, Microsoft Windows, and macOS servers.

BlastShield Orchestrator

The BlastShield Orchestrator is a cloud-based or on-prem application that provides a single-pane of glass to manage Users, Agents, Groups, and Policies. The Orchestrator can also be hosted by the customer on-prem.

BlastShield Features

- Phishing-resistant MFA authenticates users before connection
- Devices are invisible to the unauthenticated
- Simple orchestration replaces complex microsegmentation
- Agents protect each machine, application or container
- On-prem Orchestrator for air-gapped networks
- Defends against internal and external attacks
- Does not require implementation at Level 0 and 1

About BlastWave

BlastWave helps companies simplify the security stack without sacrificing performance. With BlastWave BlastShield, businesses of all sizes create a software-defined perimeter (SDP) that protects connected applications, machines, and users - making them invisible to internal and external attackers. BlastShield was rated as the fastest ZTNA solution by the Tolly Group, performing up to 34x faster than other vendors. www.blastwave.com

BlastWave