How BlastWave's Zero Trust protection saved a manufacturing plant from catastrophic downtime

Overview

A large manufacturing plant experienced a severe cyber security breach that brought its entire operation to a standstill – except for one crucial segment. As the facility's production lines stopped, one section of the plant remained unaffected, continuing to run as normal. The only difference? This part of the network was protected by BlastWave's Zero Trust Protection. This small-scale installation played a pivotal role in preventing a costly disaster across the entire operation.

The Challenge

The manufacturing plant was operating on an interconnected network where IT and OT systems were tightly integrated. Despite employing basic cyber defenses, the factory fell victim to a sophisticated cyber attack that spread quickly, disabling production lines and forcing the entire facility offline. As each line shut down, the factory stood eerily silent, except for one line still humming in production.

The Solution

Upon investigation, it became clear that the line still in operation was protected by BlastWave's Zero Trust Protection. Unlike traditional security measures, BlastWave's solution cloaked the OT systems from external discovery and blocked unauthorized lateral movement between IT and OT systems. This effectively limited the hacker's access and isolated the compromised segments from the rest of the network.

In this small trial deployment, BlastWave had implemented key protections:

Cloaking:
BlastWave made critical OT systems invisible to the attacker, preventing them from being discovered and compromised.

Segmentation:
Lateral movement between IT and OT segments was blocked, containing the attack and protecting production.

Zero Trust Architecture:
The network required strict verification at every point of access, thwarting the attack at its early stages.

The Results

While the rest of the factory sat idle for over two days, the segment protected by BlastWave remained unaffected. The financial impact of the attack was staggering – over $4.8 million in lost revenue for the areas of the plant not protected by BlastWave's Zero Trust solution. In stark contrast, the segment using BlastWave technology faced no downtime, highlighting the solution's effectiveness in preventing operational disruption.

In response to this incident, the plant's management made the strategic decision to extend BlastWave's Zero Trust Protection to their entire network. Recognizing the invaluable protection it provided, they understood that safeguarding every part of their operations was crucial to preventing future attacks.

Conclusion

This case highlights the importance of modernizing cybersecurity infrastructure, especially for industries with tightly integrated IT and OT environments. BlastWave's Zero Trust Protection can be a game-changer in defending against advanced cyber attacks. In this case, a small trial saved one part of a factory from the devastating effects of a cyber breach, reinforcing the critical need for Zero Trust architecture in today's manufacturing environments.

Don't wait for a cyber attack to take down your operations. Deploy BlastWave's Zero Trust Protection today and safeguard your network from threats. Contact us at www.blastwave.com/contact to learn more.

v20250625

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