BULLWALL

RANSOMWARE ATTACKS CAN SEVERLY DAMAGE THE MANUFACTURING INDUSTRY, LEADING TO COSTLY DOWNTIME AND PRODUCTION DELAYS

Ransomware attacks can have devastating effects on the manufacturing industry, impacting operations, finances, and reputation. These attacks can halt production lines, disrupt supply chains, and cause quality control issues, leading to significant downtime and defective products. Financially, companies may face ransom payments, revenue loss from missed production deadlines, substantial recovery costs, and increased insurance premiums.

THE RISK

61%
of manufacturing and production organizations experienced ransomware attacks

156%
increase in ransomware attacks against manufacturing between 2019 and 2020

70%
of those attacked reported that their operations were significantly impacted

THE BULLWALL SOLUTION

Data security within manufacturing is essential to ensure uninterrupted production continues around the clock. However, with an increasing number of entry points, and preventative solutions unable to keep up with the different variants of ransomware and their innovative delivery methods, sooner or later ransomware will slip through.

Leveraging 28 detection sensors and machine-learning capabilities to instantly detect illegitimate encryption and exfiltration, BullWall is the last line of defense against ransomware that has breached preventative security solutions.

The solution operates by automatically quarantining the infected user(s) and isolating the attack so that it can't spread further. By stopping the encryption in seconds BullWall ensures continuous operation with zero downtime.

> *Experiencing a ransomware attack was a wake up call for our entire organization. It made us realize the importance of having a containment solution.*
>
> - CISO of Large US Manufacturing Company

DETECT

BullWall uses 28 sensors and machine learning to monitor file activity and identify abnormal events.

ISOLATE

BullWall stops active attacks, quarantine the infected user & device, and protects your critical IT infrastructure.

REPORT

BullWall notifies your IT team within seconds and provides a report of compromised devices and files to expedite recovery.

NO ENCRYPTION, NO RANSOM

BullWall eliminates ransom demands by stopping malicious encryption in seconds.

NO EXFILTRATION, NO EXTORTION

BullWall minimizes extortion and protects PII by preventing malicious data exfiltration.

### NO DOWNTIME, NO WORRIES

BullWall thwarts and isolates attacks before the damage can spread, so there's no downtime.

THE TRUSTED PARTNER IN MANUFACTURING

BullWall is currently protecting 50,000+ manufacturing professionals around the world, enabling them to:

- Ensure continuity of operations and production
- Avoid costly downtime, ransom payments and recovery costs
- Stop the exfiltration of sensitive information
- Avoid increased insurance premiums and loss of reputation
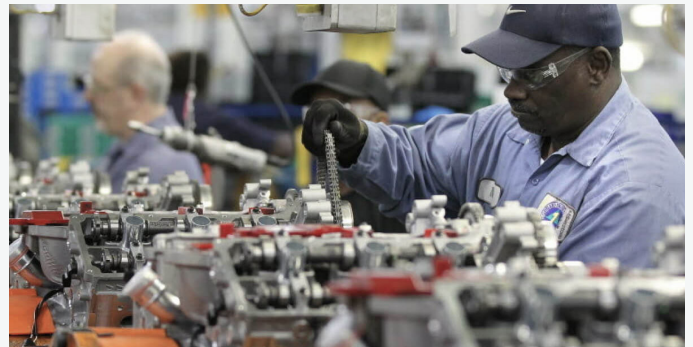
THE ONLY SOLUTION OF ITS KIND

BullWall is agentless, lightweight and designed to be easily implemented and integrated into your existing security solutions. Entirely automated, the system requires no hands-on monitoring and will respond automatically to any ransomware attack, be it a known strain or a zero-day attack.

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting critical IT infrastructure from ransomware. We provide rapid containment of active attacks, and safeguard servers by preventing unauthorized intrusion.

Learn more at www.bullwall.com.

BULLWALL

Version 1.0_24