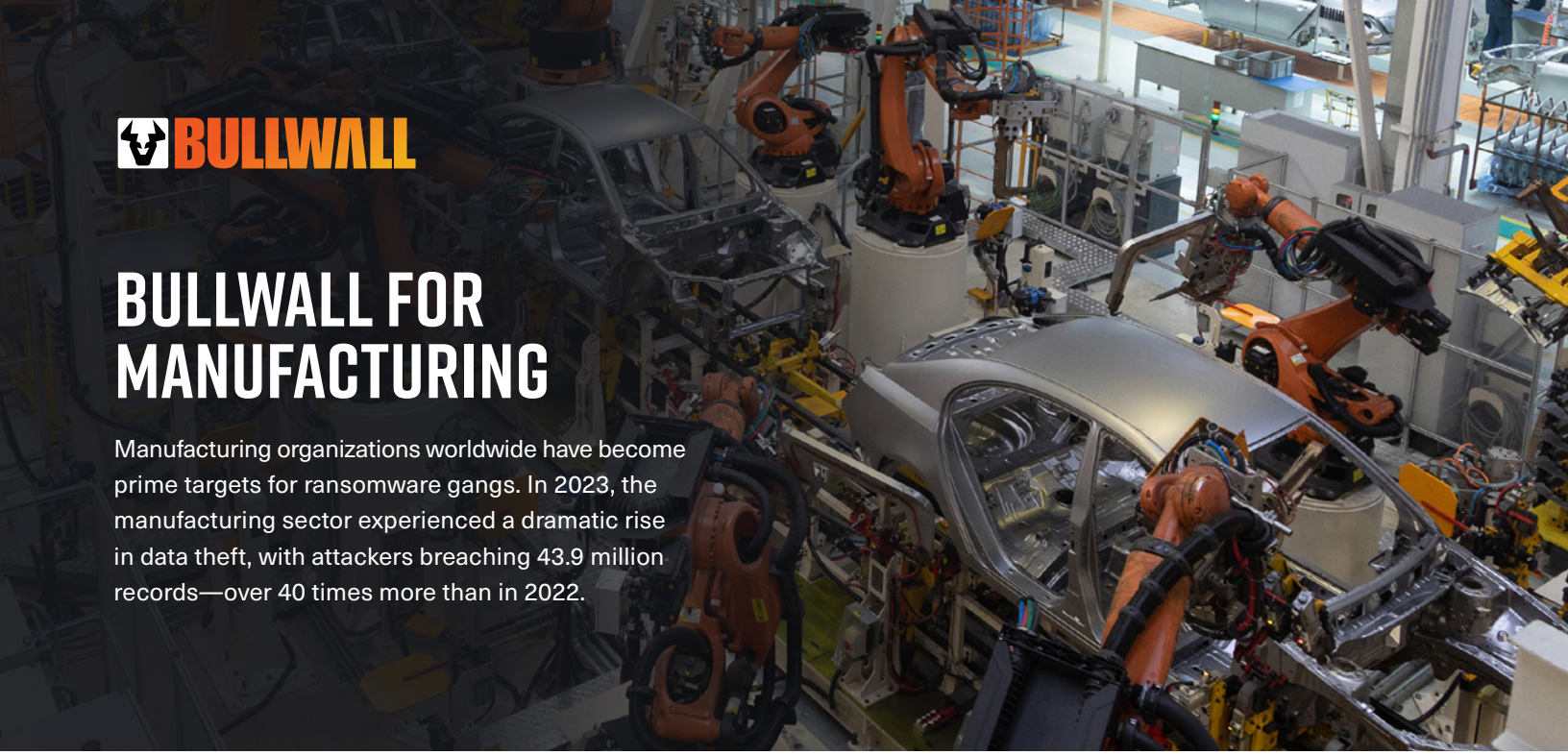


BULLWALL

BULLWALL FOR MANUFACTURING

Manufacturing organizations worldwide have become prime targets for ransomware gangs. In 2023, the manufacturing sector experienced a dramatic rise in data theft, with attackers breaching 43.9 million records—over 40 times more than in 2022.

THE CONSEQUENCES OF RANSOMWARE ARE WIDER THAN SIMPLY THE FINANCIAL IMPACT.

The average cost to recover from a ransomware attack in the manufacturing industry increased from $1.08 million in 2023 to $1.67 million in 2024. However, these incidents not only result in substantial financial losses but also disrupt critical production processes, underscoring the urgent need for enhanced cybersecurity measures within the manufacturing sector.

WHY BULLWALL?

BullWall provides a specialized ransomware containment solution designed specifically for the manufacturing industry, where operational continuity and data integrity are critical. By quickly detecting and halting ransomware attacks in real-time, BullWall ensures that production lines remain unaffected and sensitive intellectual property, such as product designs and manufacturing processes, is protected.

This rapid response capability helps manufacturers maintain business continuity, mitigate financial losses, and preserve their reputation in an increasingly hostile cyber threat landscape.

$1.67M

was the average recovery cost per attack for the manufacturing industry in 2024

$1.9B

was the overall cost of downtime suffered by the industry in 2023

Sophos News
Comparitech

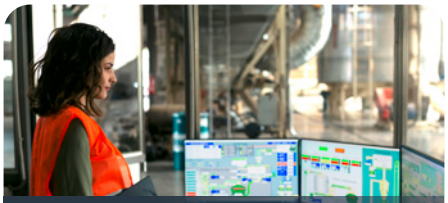
> ***Experiencing a ransomware attack was a wake-up call*** *for our entire organization. It made us realize the importance of having a containment solution.*
>
> **CISO**
> of a Large US Manufacturing Company

HOW MANUFACTURING ORGANIZATIONS BECOME A RANSOMWARE TARGET

PHISHING EMAILS & SOCIAL ENGINEERING ATTACKS

60%

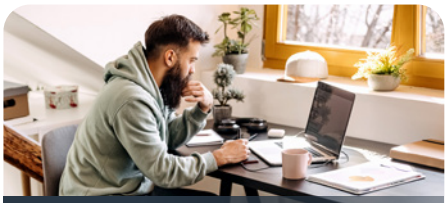
With phishing emails targeting 6 in every 10 email addresses, there's never been a more prudent time to secure this method of entry.



EXPLOITING VULNERABILITIES IN LEGACY SYSTEMS

47%

of cyberattacks in the manufacturing sector originate from unpatched vulnerabilities.



RANSOMWARE VIA WEAK REMOTE ACCESS POINTS

20%

of ransomware incidents in industrial sectors in 2024 involved exploiting remote access tools, such as VPN vulnerabilities and remote desktop protocols.

THE IMPACT

When attacked, organizations can't simply measure the attack's impact by the ransom requested. Many other factors come into play, such as the ability to stay operational and the daily impact a loss of production has on the organization's long-term future.

OPERATIONAL DISRUPTION

Ransomware can encrypt critical systems, halt production lines, disrupt supply chains, and cause significant downtime. This downtime can lead to missed deadlines, lost revenue, and reputational damage.

FINANCIAL LOSSES

The organization may face direct costs such as ransom payments, legal fees, IT recovery expenses, and indirect costs like lost sales, regulatory fines, and increased insurance premiums.

DATA SECURITY & COMPLIANCE RISKS

Ransomware attacks often involve data theft, exposing sensitive customer, employee, or intellectual property information. Data theft can lead to legal consequences, compliance violations, and a loss of customer trust.

WHAT IS RANSOMWARE RESILIENCE?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.

PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.

CONTAINMENT

Minimize disruptions to business operations when ransomware breaches preventative security measures, and streamline your recovery efforts.

RECOVERY

Resilient organizations rebound swiftly, minimizing downtime and emerging stronger.

BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

Phishing emails are a bad actor's friend. Cybercriminals leverage phishing emails to target the most vulnerable part of the security chain—the human element.

BullWall steps in, containing attacks instantly without endpoint installations, ensuring no damage is done when a malicious link is clicked by mistake.

Ransomware exploits weaknesses in critical manufacturing systems such as supply chain management systems and industrial control systems.

BullWall addresses urgent gaps left by traditional security solutions.

For cybercriminals, shutting down an organization's preventative security before launching an attack is their preferred approach.

BullWall stops unauthorized access and lateral movement.

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware.

Learn more at www.bullwall.com.

BULLWALL