BULLWALL

CASE STUDY

STAR PIPE PRODUCTS STRENGTHENS RANSOMWARE RESILIENCE TO PROTECT MANUFACTURING OPERATIONS

STAR PIPE PRODUCTS

Industry
Manufacturing

Location
United States

Products
BullWall Ransomware Containment
BullWall Virtual Server Protection
BullWall Server Intrusion Protection

15
Regional Distribution Centers

3,000+
Employees

1M+
Sq. Ft. of Storage

MANUFACTURING OPERATIONS ARE NO LONGER OFF-LIMITS TO RANSOMWARE

Star Pipe Products is a global manufacturer and supplier of ductile iron pipe fittings, accessories, and municipal castings, supporting critical infrastructure projects across North America. With 15 regional distribution centers, more than 3,000 employees worldwide, and over one million square feet of storage capacity, uninterrupted operations are essential to meeting customer demand and industry standards.

Like many manufacturing organizations, Star Pipe operates a complex IT environment supporting distributed facilities, production systems, and logistics workflows. While the organization does not fall under strict regulatory mandates such as HIPAA or PCI, leadership has remained focused on cybersecurity best practices to protect intellectual property, operational systems, and business continuity.

That focus was shaped by experience. Several years ago, Star Pipe suffered a ransomware attack that encrypted shared files across the environment. While the incident did not shut down production, recovery was slow and highly manual. Documents were restored by scanning physical records back into digital systems—a process that took approximately three months.

"That incident was a wake-up call," said Jeff Greer, Director of IT at Star Pipe Products. "It didn't stop the business, but it showed how long recovery can take and how disruptive ransomware can be if systems aren't fully protected."

PREVENTION ALONE IS NOT ENOUGH FOR OPERATIONAL CONTINUITY

Following the attack, Star Pipe significantly expanded its cybersecurity posture. The organization deployed layered security controls, including MFA, firewalls, email gateways, EDR/XDR, cloud backups, phishing simulations,

and regular security testing. A cross-functional cybersecurity team was established, and frameworks such as NIST CSF and ISO 27001 were leveraged to guide ongoing improvements.

DESPITE THESE INVESTMENTS, LEADERSHIP RECOGNIZED AN ONGOING GAP: **PREVENTION AND BACKUPS REDUCE RISK, BUT THEY DO NOT STOP RANSOMWARE ONCE IT EXECUTES.**

"There's always the concern that restoring from backups puts the same malicious code right back into the environment," Greer explained. "Prevention is far less work than recovery, but prevention alone doesn't guarantee resilience."

At the same time, ransomware was becoming a board-level concern. Senior leadership wanted assurance that a ransomware incident would not halt manufacturing operations or result in extended downtime across distributed facilities. Cyber insurance expectations were also evolving, with insurers increasingly focused on an organization's ability to reduce impact—not just detect threats.

The conversation shifted from recovery planning to Ransomware Resilience—specifically, how to contain an active attack and maintain operational continuity.

CONTAINMENT AS THE FOUNDATION FOR RANSOMWARE RESILIENCE

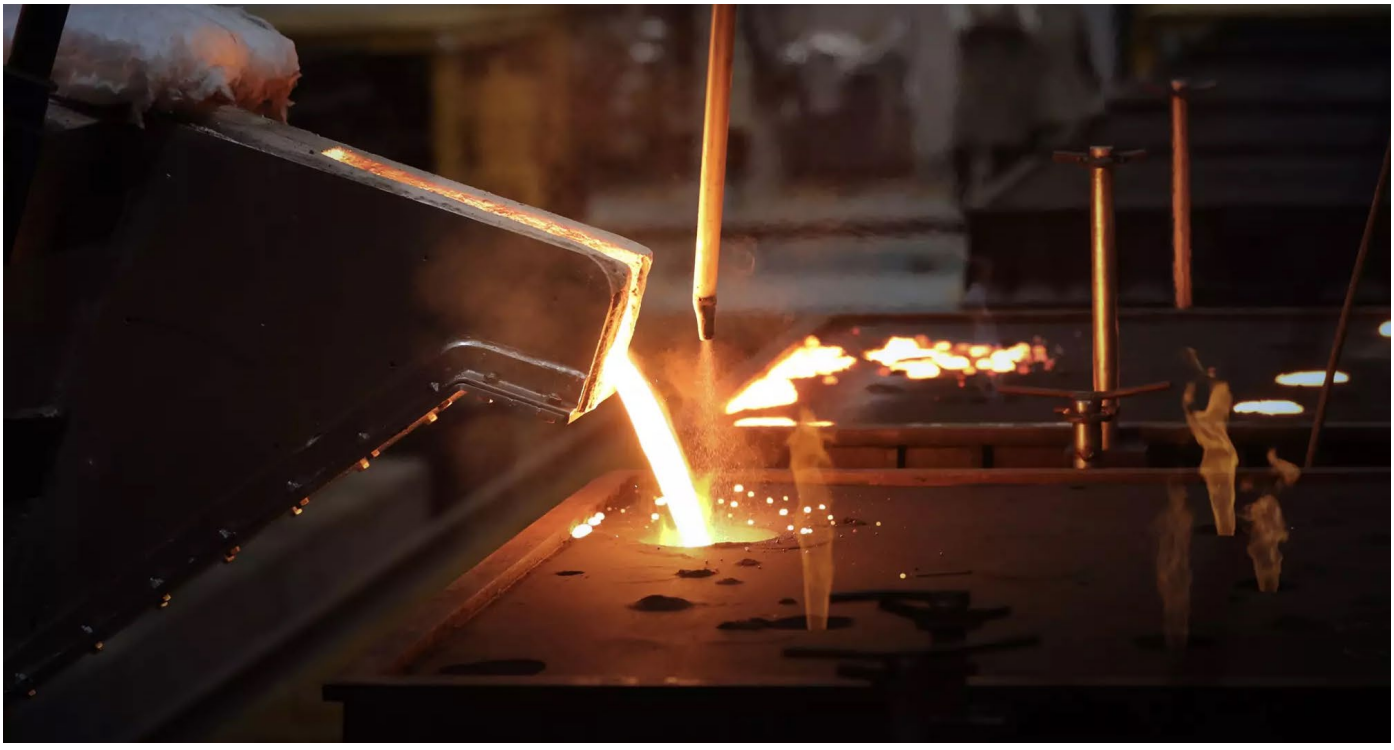
Star Pipe was introduced to BullWall through a trusted technology partner. Initially, the organization took a measured approach, but growing concern around ransomware impact accelerated the decision.

"We were focusing on disaster recovery, and leadership wanted something stronger for ransomware," said Greer. "Backups and DR aren't ransomware recovery. When the focus turned to containment, BullWall made sense."

Star Pipe deployed BullWall Ransomware Containment, BullWall Server Intrusion Protection, and BullWall Virtual Server Protection to serve as a last line of defense within its existing security stack. Closing a critical gap between prevention and recovery.

"The BullWall team knew the product inside and out, and we were able to move through setup efficiently," Greer noted. "Now it's about tuning and making it fit exactly how we want as part of the broader environment."

BullWall now provides Star Pipe with automated containment of active ransomware and malicious activity, reducing the risk that an attack could spread, encrypt critical systems, or disrupt operations. Instead of relying solely on alerts or post-incident recovery, the organization has strengthened its ability to maintain operational continuity if an attack gets through.



"It's about making sure the business keeps running," Greer said. "Prevention is important, but containment is what protects operations when something gets through."

CONTAINMENT AS THE FOUNDATION FOR A MORE RESILIENT MANUFACTURING ENVIRONMENT

Today, Star Pipe Products operates with greater confidence that ransomware will not translate into prolonged downtime. With BullWall in place, the organization has strengthened its overall cybersecurity maturity while aligning with evolving cyber insurance and risk expectations.

For manufacturing organizations where uptime, safety, and continuity are critical, Star Pipe's experience underscores a growing reality: Ransomware resilience requires more than prevention...it requires containment.

> *We were focusing on disaster recovery, and leadership wanted something stronger for ransomware. Backups and DR aren't ransomware recovery.* ***When the focus turned to containment, BullWall made sense.***
>
> ***Jeff Greer***
> *Director of IT*
> *Star Pipe Products*

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware. Our focus on the latest ransomware tactics uniquely addresses critical gaps left by other security solutions. By delivering server-based protection without an endpoint agent, BullWall keeps critical IT infrastructure secure and operational during the core stages of an attack – before, during and after.

Learn more at www.bullwall.com.

BULLWALL