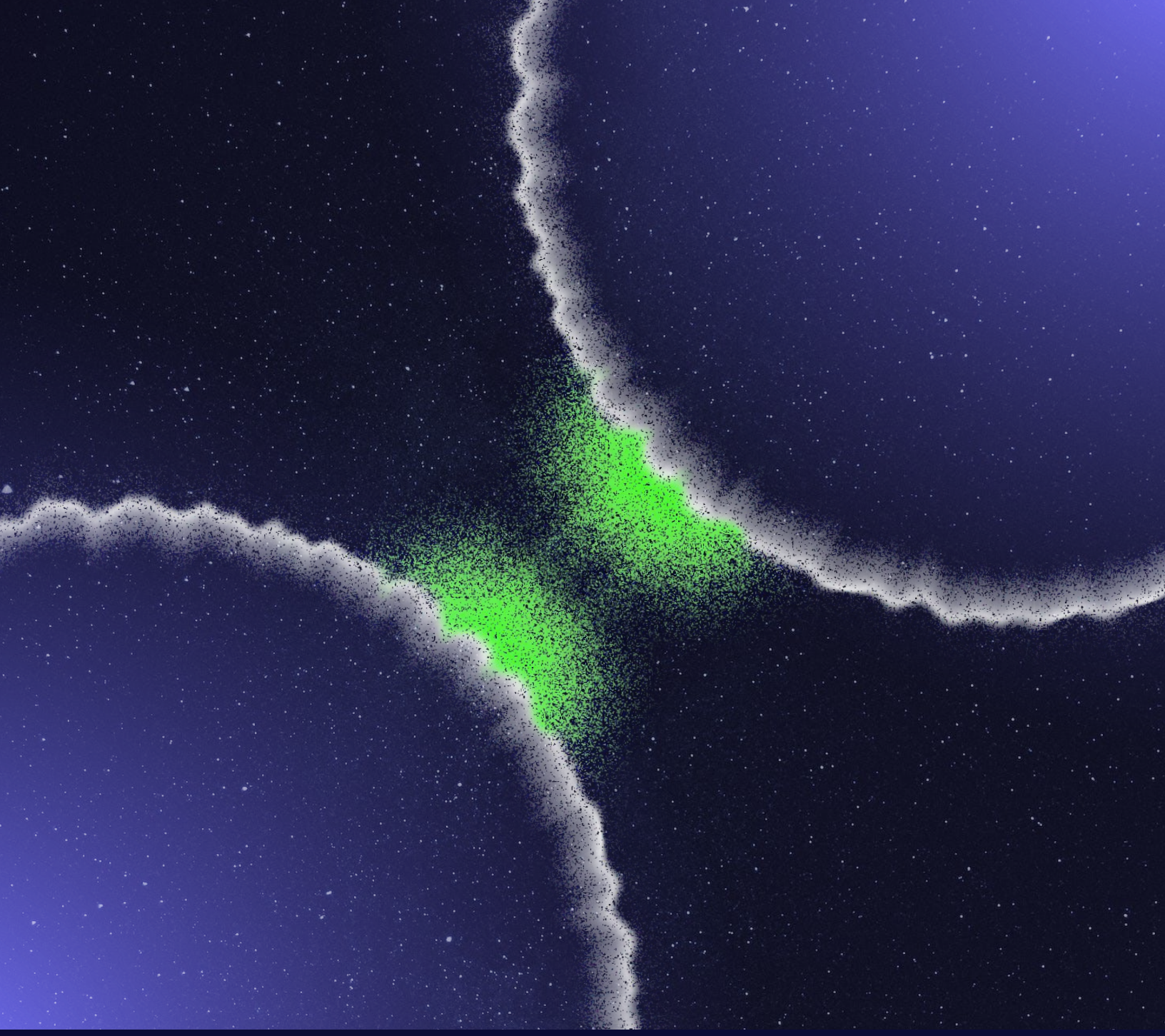

PROTECTING THE PRODUCTION LINE: PROACTIVE CYBERSECURITY SOLUTIONS TO DEFEND THE GLOBAL MANUFACTURING INDUSTRY FROM RISING THREATS

CENTRIPETAL

The manufacturing industry stands as a critical pillar of the global economy, and consequently has become an increasingly attractive target for cybercriminals. The sector's heavy reliance on interconnected technologies and the prevalence of legacy systems have exposed significant vulnerabilities.

In 2023, about a quarter of all cyberattacks worldwide involved manufacturing companies. Ransomware, one of the most common types of cyberattacks in this sector, hit almost all subsectors, targeting metal products and automotive productions more frequently. North America accounted for 40 percent of ransomware attacks on industrial organizations and infrastructures worldwide, and in 2022, the global average cost per industrial data breach was around 4.73 million U.S. dollars.

As cyberattacks become more sophisticated, manufacturers must adopt proactive, intelligence powered cybersecurity solutions to protect their operations and data. This document explores the key threats facing the manufacturing industry and underscores the urgent need for advanced cybersecurity measures.

The Growing Threat Landscape

Manufacturing remains among the most targeted industries by cyberattacks in the world. In 2023, the sector faced several high-profile attacks, including a devastating incident at Clorox, which resulted in a $356 million loss due to production declines.

Similarly, a hack involving a business partner of Applied Materials cost the company $250 million. These examples illustrate the severe financial impact of cyberattacks on manufacturers.

The manufacturing sector's low tolerance for downtime and its reliance on interconnected technology make it a prime target for cybercriminals seeking financial gains through extortion. Extortion was noted as the primary impact in 27% of cyberattacks on the sector.

Challenges the Manufacturing Sector Faces

Several factors contribute to the manufacturing industry's vulnerability to cyberattacks:

01

Legacy Systems

Many manufacturers still rely on outdated industrial technologies, which lack modern security features.

02

Interconnected Technology

The integration of IoT devices and automated systems creates numerous entry points for attackers.

03

Supply Chain Vulnerabilities

Weaknesses in the supply chain can disrupt operations downstream. Manufacturers depend on timeliness and reliability of suppliers. If the suppliers were to be impacted by a cyberthreat, it is likely that the manufacturing process could be severely hampered.

04

Credential Harvesting

Credential harvesting has the largest impact on the manufacturing sector, highlighting threat actors' interest in high-value data. X-Force observed a 266% rise in infostealing malware designed to obtain credentials for emails, social media, messaging apps, and banking details related to this industry. This trend shows that threat actors are continuously innovating to access user identities through credentials.

The Importance of Intelligence Powered Cybersecurity in Manufacturing

Effective security is only achievable if it is based on the latest knowledge of who and what is attacking your network. This information is available from threat intelligence vendors and can be used to enable real time security protection. This approach is transformative for any organization and ends the reactionary approach to security that many manufacturing companies struggle with, leading to some clear benefits.

Proactive Defense

Traditional cybersecurity measures are often reactive, addressing threats only after they have infiltrated the network. Intelligence powered solutions, however, shift the paradigm to proactive defense. By leveraging real-time threat intelligence from a global network, these solutions identify and neutralize potential threats before they can cause harm. This proactive approach provides manufacturing companies with a robust security posture, protecting critical production processes and sensitive data.

Enhanced Visibility

Intelligence powered cybersecurity offers enhanced visibility into potential threats, enabling analysts to monitor and analyze vast amounts of data in real-time. This visibility is crucial for anticipating and mitigating risks. Organizations using intelligence powered solutions have reported a 50% reduction in time to detect threats and improved incident response times. For manufacturing companies, this means quicker responses to potential threats and a more secure environment for proprietary information and production systems.

Efficiency and Cost-Effectiveness

Deploying an intelligence powered cybersecurity solution can significantly reduce the operational burden on IT teams. Automated threat detection and response capabilities minimize the need for manual intervention, allowing IT professionals to focus on more strategic tasks. Additionally, these solutions offer a cost-effective alternative to building an extensive in-house security infrastructure — a challenge that manufacturing companies often face.

01

Cost Savings

A typical manufacturing organization can save, on average, $1-2 Million on their cybersecurity and networking cost by deploying intelligence powered solutions.

02

Resource Allocation

IT teams can reduce time spent on threat analysis by 80%, reallocating resources to more critical areas.

By adopting intelligence powered cybersecurity solutions, manufacturing companies can enhance their defense capabilities, improve efficiency, and achieve significant cost savings.

Three Strategic Steps to Maximize the Potential of Intelligence Powered Cybersecurity for the Manufacturing Sector

Manufacturing remains among the most targeted industries by cyberattacks in the world. In 2023, the sector faced several high-profile attacks, including a devastating incident at Clorox, which resulted in a $356 million loss due to production declines. Similarly, a hack involving a business partner of Applied Materials cost the company $250 million. These examples illustrate the severe financial impact of cyberattacks on manufacturers.

Utilize the Latest Threat Intelligence for Real-Time Protection

01

Leverage the latest threat intelligence from the cybersecurity community and industry to enhance your defensive posture.. Blocking malicious and reconnaissance traffic before it enters the network eliminates threats before they can cause harm, ensuring the protection of sensitive production data and operational integrity.

Collaborate with Cybersecurity Experts Using AI and Human Intelligence

02

The scale of cyber protection is now so vast that leveraging industry-wide expertise is essential. Partnering with cybersecurity experts who utilize powerful AI-enabled tools and deep industry knowledge can significantly bolster your defenses against a wide array of threats. Manufacturing companies can benefit immensely from these collaborations, enhancing their security measures without overextending their resources.

Join a Cybersecurity Data Sharing Community

03

Security incidents in one manufacturing company can often occur in others as well. By sharing threat data, companies can collectively improve their defenses. Geographic and sector-specific communities can exchange experiences, indicators of compromise (IOCs), techniques, and resolutions. Sharing threat data is increasingly becoming a regulatory requirement. Immediate strategic gains can be achieved by working with experts who can interpret and rapidly deploy community learnings, strengthening the overall cybersecurity posture of manufacturing companies.

The Solution: Proactive Protection with CleanINTERNET®

Centripetal's CleanINTERNET® solution presents a tailored approach to the unique needs of manufacturing companies. In an environment where time-sensitive operations and proprietary documents are under continuous attack, CleanINTERNET® harnesses real-time threat intelligence from a global network, providing visibility into potential threats before they can affect your systems. This technology serves as a protective barrier, ensuring the security of sensitive information.

> "CleanINTERNET® is an excellent final layer of security for public-facing networks. We look at it as a necessary insurance policy. When you turn on CleanINTERNET®, it gets used thousands of times a minute."
>
> CENTRIPETAL CUSTOMER

CleanINTERNET® is an intelligence powered security solution that utilizes high-performance computing technology, patented software algorithms, and highly skilled security analysts to offer a cost-effective alternative protection strategy. Manufacturing companies that have adopted CleanINTERNET® are impressed by its comprehensive capabilities, which far exceed basic intelligence feeds. Achieving a similar security posture independently would be financially unfeasible.

CleanINTERNET® revolutionizes cybersecurity by prioritizing threat intelligence and shifting from reactive to proactive defense. This enhances the efficiency and effectiveness of security teams. With advanced shielding technology, CleanINTERNET® eliminates the majority of threats and mitigates the impact of any malicious code that breaches defenses. The technology blocks malicious network attempts from known sources, prevents outbound activity to malicious domains, and eliminates unnecessary reconnaissance traffic from your network.

By implementing CleanINTERNET®, manufacturing companies can quickly bolster their cyber defenses without significant financial investment or the need to expand their cyber analyst teams. This solution greatly reduces the number of security events, allowing IT teams to focus on maintaining production and operational efficiency with greater confidence.

Time Is Of The Essence For The Manufacturing Industry

For manufacturing companies, embracing intelligence powered cybersecurity solutions is not just an option; it's a necessity. By being proactive, you can transform your defenses and ensure robust protection for your sensitive data and production processes. Take the lead in cybersecurity innovation and safeguard your operations against the threats of today and tomorrow.

As cyber threats evolve, vigilance is crucial. Manufacturing companies must understand both the expanding attack surface and the increasingly malicious tactics of cybercriminals. Strengthening cyber preparedness protects your organization's future success.

centripetal.ai