

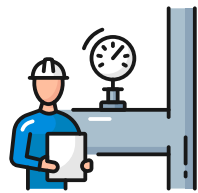


INDUSTRIAL MANUFACTURING CYBERSECURITY

Security of INDUSTRIAL MANUFACTURING organizations is a serious global issue.
Some eye-opening stats about cybersecurity in Manufacturing Industry.

33.8%

of industrial control systems (ICS) were attacked in the first half of 2021



34%

of all malware detections in manufacturing during 2020 was attributed to the Morto worm

47%

of attacks on manufacturing were caused due to vulnerabilities that victim organizations had not yet or could not patch



\$ 300 K

An average cost of an IoT device cyberattack for a manufacturing organization



THE 2ND

most-targeted industry in 2020 was manufacturing



"Ransomware operators shut down two production facilities belonging to a European manufacturer after deploying a relatively new strain that encrypted servers that control a manufacturer's industrial processes"

REFERENCES

[How a VPN vulnerability allowed ransomware to disrupt two manufacturing plants](#)

[Top Cyber Security Statistics, Facts & Trends in 2022](#)

[IBM Report: Manufacturing Felt Brunt of Cyberattacks in 2021 as Supply Chain Woes Grew](#)

[Industrial IoT Cybersecurity: Top Questions, Key Insights](#)

HOW BINARE CAN HELP?

Binare can deploy its solution on-premise of manufacturing organizations:

- Our solution is scalable, flexible and built with best practices in software design and architecture
- Binare can customize the way its solution integrates into manufacturing organization's workflows and existing systems
- Binare can customize the type of analysis/results needed for manufacturing organization
- Binare can customize the reporting formats and layouts