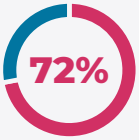
INDUSTRY TRENDS

Industrial Manufacturing Cybersecurity and Operational Resilience

NOZOMI NETWORKS

Manufacturers are on the road to Industry 4.0, business needs have demanded it—but are they prepared for the exponential risk?



2022:

72% of all manufacturers have a digital transformation roadmap

The Aptean 2022 Manufacturing Forecast

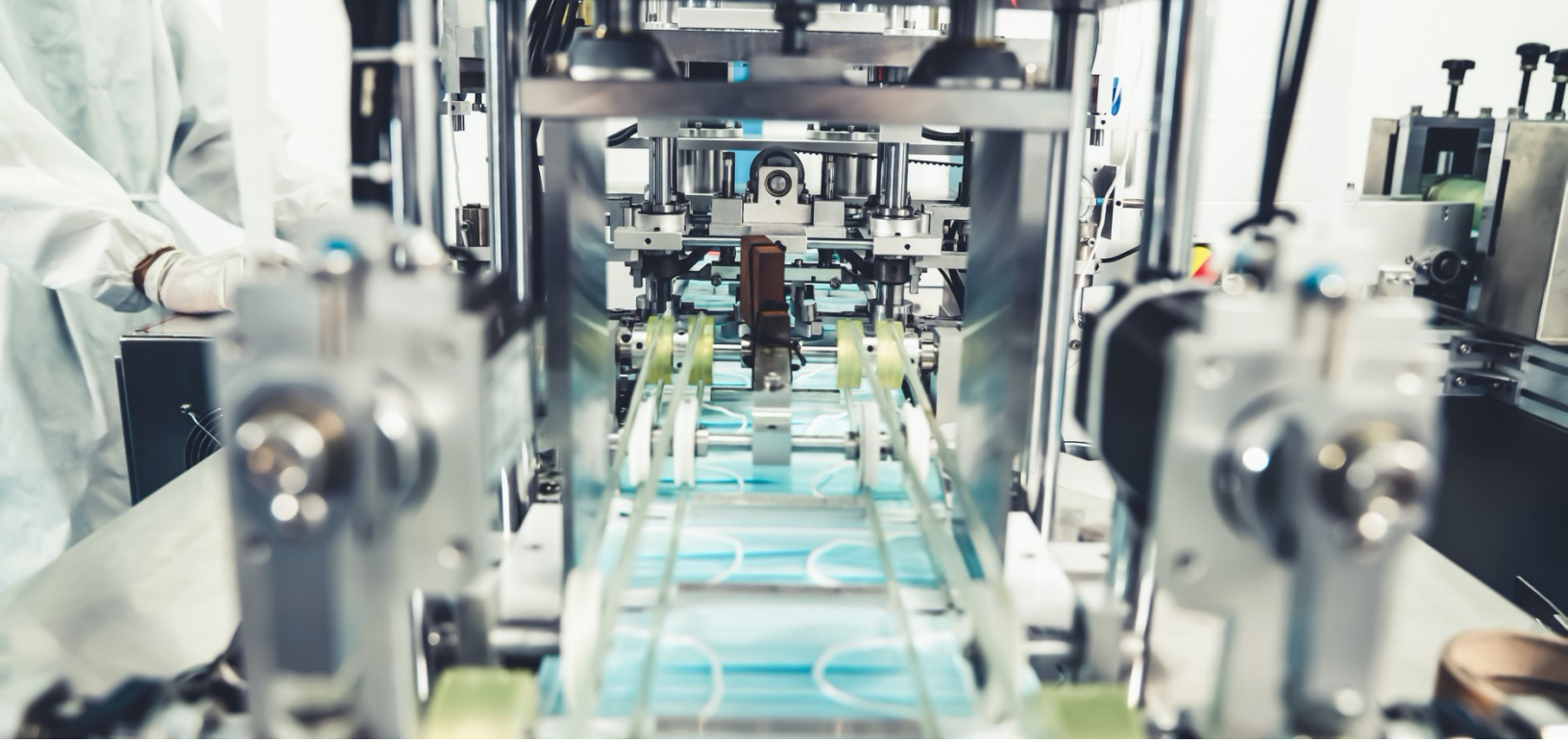
Industry 4.0 is no longer a goal; it is a reality. Workforce shortages, skill gaps and supply chain disruptions drive an inescapable need for efficiency. There is also a fundamental shift in the convergence of IT and OT systems, where unified visibility and risk management are now required.

As manufacturers begin to connect disparate systems, integrate more assets and systems, and bring in IoT to optimize, there is a significant risk of operational downtime and exponential exposure to new cyber threats.

The Need for Efficiency

45% of manufacturing executives expect efficiency improvements from IoT investments.[1] With IoT, manufacturers can obtain data-driven insights to create efficiencies that were never previously possible. The movement to smart factories is expected to improve competitiveness and help address workforce shortages and supply chain interruptions. To gain the needed efficiencies, manufacturers need to address the security challenges of both legacy equipment and IoT proliferation, ultimately improving the cybersecurity and resilience oversight of all factory assets and systems.

1. Deloitte 2022 Manufacturing Industry Outlook



The Need for Operational Resilience

Operational resilience has never been more critical. The competitive landscape within manufacturing, along with recent supply chain disruptions, puts immense pressure on factories to improve uptime. Assessing cyber and operational risk for manufacturing facilities is of paramount importance to boards of directors. The ability to quickly detect failures or potential failures and then respond to them in real time is challenging without visibility into OT environments. Therefore, to improve operational resilience, it is essential that while factories are digitalizing, cyber and operational risk are continuously assessed and mitigated.

The New Cyber Threat Landscape

Manufacturers are under unprecedented attacks by cyber threat actors. According to Deloitte, most U.S. manufacturers reported phishing or ransomware security incidents.[2] Ransomware is a threat to manufacturers because it can shut down production and disrupt day-to-day operations. As factories transform, their attack surface is exponentially increasing, requiring security visibility into all IT, OT and IoT systems across all facilities.

2. Deloitte 2022 Manufacturing Industry Outlook

Nozomi Networks reduces cyber risk and operational downtime by providing visibility and security for OT, IT and IoT systems across all facilities.

Accurate detection of cyber threats, risks and anomalies improves operational resilience.

Visibility

You can't protect what you can't see. Nozomi Networks automates asset inventory creation, eliminating blind spots and revealing assets others don't see. **It provides accurate and extensive information on all OT, IoT and IT assets from all systems**—no matter their age, vendor or function.

Reliability

Improving operational reliability requires real-time situational awareness. By learning your factory's normal network patterns and manufacturing processes, our solution identifies anomalies**. We help you act before equipment failure, unusual variable values, or network stability issues impact production uptime or quality**.

Risk Reduction

We give you confidence regarding the state of your **operations thanks to our 24/7/365 monitoring and deep OT capabilities**. You are informed of cyberattacks, vulnerabilities and risks to reliability. Pinpoint alerts and actionable insights help you mitigate cyber and operational threats before they cause harm.

For more information on Nozomi Networks' solutions for manufacturers, visit nozominetworks.com/solutions/manufacturing/