The Benefits of Network Monitoring for Industrial Automation
Industry 4.0

The drive to increase productivity and reduce costs in manufacturing environments has led to an exponential increase in the adoption of automation on plant floors. Commercial-off-the-shelf (COTS) computers mostly running outdated software communicate with legacy control systems interact with field sensors and actuators to drive the production process. On top of these core technologies, intelligent devices are often employed to collect, exchange and analyze data to produce valuable business analytics.

The integration of computation, networking, and physical processes is what characterized the 4th industrial revolution we are in also known as Industry 4.0 or the Industrial Internet of Things (IIoT). Despite the clear business advantages, this trend also led to manufacturing networks which are more complex and highly heterogeneous, and as a result are operating with an increased risk of industrial specific flaws. These flaws pave the way to cyber and operational incidents, as endured by Norsk Hydro in 2019[1], several car manufacturers in 2017[2], and by hundreds of plant floors every day.

Today, industrial assets owners have little to no visibility into existing industrial threats and flaws, and therefore no way to anticipate, analyze and respond to incidents. Providing visibility into industrial networks is the first step to gain full control of the environment. This whitepaper shows how the use of network monitoring technology in manufacturing networks brings tremendous value to both information technology (IT) and operational technology (OT) teams.
Lately, a lot of attention has been inevitably captured by the many cyberattacks occurring in the industrial automation world from the Wannacry ransomware and the Petya/NotPetya wiper to the LockerGaga malware that targeted Norsk Hydro. The risk of cyberattacks is rising, and the implementation of cybersecurity measures should be high on the agenda of industrial asset owners. When choosing a strategy to implement, guidelines such as the NIST Cybersecurity Framework and IEC 62443 can provide valuable advice on how to improve the overall cybersecurity of industrial networks.

However, cyberattacks are by far not the most imminent threats to the manufacturing industry. The truth is that, despite the noise from the media, the likelihood of a successful attack against industrial control systems (ICS) is relatively low. On the contrary, cyber incidents happen daily. Cyber incidents include small to major network or process disruptions due to misconfigurations, erroneous commands and operations, software errors and device failures which are not intentional, but nevertheless impact the asset owner’s bottom line.

To effectively protect the network and avoid downtime, asset owners must be able to detect all these threats in a timely manner. The figure below provides a good overview of the industrial automation threat landscape, including the frequency and impact of threats and problems.
The examples of operational and networking threats presented above are detected daily at most of our manufacturing customers. The statistics below represent the actual proportion of cybersecurity vs. networking and operational threats experienced by our global customer base in the last seven years.

Network and operational threats outweigh attacks and intrusion attempts ten to one.

Note that the cybersecurity statistics above are limited to intrusion attempts and attack, and do not include for instance, weak security implementations such as firewall misconfiguration and the use of insecure devices, protocols and services, which are still extremely common in the industry. As these statistics show, the most imminent threats to manufacturing processes stem from the lack of infrastructural resilience, or in other words, the lack of network cyber resilience, of which security is only a part.
Being cyber resilient means being able to identify and quickly recover from any threat to operational continuity. Manufacturing operators can save considerable time, effort and money by detecting and fixing existing and emerging problems and threats before they cause disruptions, thereby creating a healthier and more robust infrastructure. Real cyber resilience comes from the effective and continuous application of four activities:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assess</strong></td>
<td>Gather all device data to determine the current security and operational state of the network and develop a complete map of the network, including asset zones and communication flows. This activity aligns with the Identify function of the NIST Cybersecurity Framework.</td>
</tr>
<tr>
<td><strong>Secure</strong></td>
<td>Deploy security controls to limit what is allowed on the OT network in real time, while also responding to failed policy conditions with automated network segmentation policy enforcement. This activity corresponds with the Protect Function of the NIST Cybersecurity Framework.</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>Continuously monitor the infrastructure to catch the early symptoms of emerging problems and threats. This activity corresponds to the Detect function of the NIST framework.</td>
</tr>
<tr>
<td><strong>Respond</strong></td>
<td>When a threat is detected, apply the appropriate corrective measures to restore the desired system operation and the network’s cyber resilience, as indicated by NIST’s Respond and Recover functions.</td>
</tr>
</tbody>
</table>
Forescout’s ICS network monitoring solution, eyeInspect (formerly SilentDefense), continuously monitors OT networks to enhance the cyber resilience of industrial networks. It’s ideal for a manufacturing environment, as it delivers value and protection for every “ingredient”: network, process, and security.

Our solution provides fundamental contributions in all four key cyber resilience activities.

- Creates a complete asset inventory and network baseline, automatically and passively
- Provides accurate device fingerprinting for all major ICS vendors, including installed firmware and device modules, and allows the export of all collected information
- Delivers automated impact-based security and operational risk scoring to effectively guide the prioritization of patching and protection
- Identifies existing networking and operational problems, pinpointing weak spots and current inefficiencies
- Presents all information in an intuitive, interactive network map
Monitor

- Provides real-time network visibility through visual network analytics widgets and dashboards, to quickly spot trends and anomalies
- Automatically creates a baseline of current network communications that operators can validate and use as a whitelist for anomaly detection
- Features deep packet inspection for all common industrial protocols and vendors, with patented technology to detect hidden threats
- Combines anomaly detection with an industrial threat library (ITL) of over 2,400 ICS-specific threat checks, including networking, operational and security threats at different stages of the kill chain
- Integrates with SIEM solutions and other logs collectors in a matter of minutes, to provide the operator with a unified security view

Respond

- Alerts in real time if a threat or problem is detected to enable immediate response and mitigation
- Includes rich contextual alert information, such as source and target details and a PCAP of the suspicious event, for effective root cause analysis
- Provides quick diagnostics and troubleshooting support, saving operators from the tedious task of going through system and network logs
- Guides the incident prioritization and response process by indicating alert severity, operator profile best suited to follow up and suggested next steps
- Supports visual forensic analysis with configurable widgets for in-depth search, filter and analysis of historical data and logs
- Visualizes incident details on the interactive network map, providing a bird’s eye view of its spread
Secure

- Monitors down to the process values to help ensure security policies are being followed
- Continuously assesses device security posture to control what’s allowed on OT network segments in real time
- Automates response actions if a device fails any policy condition
- Validates and automates network segmentation efforts and firewall policy changes
- Enables predictive maintenance by providing early indicators of device misconfiguration, malfunction or failure

eyeInspect is deployed in a matter of hours and provides immediate value with its out-of-the-box capabilities, delivering immediate return on investment (ROI). Its scalable architecture lets operators monitor distributed, remote production environments from a single screen.

eyeInspect can be used in multi-vendor environments, as it natively supports all major ICS vendors and protocols, including proprietary ones. Custom solutions are also available for Profinet and building automation networks.
Benefits

The benefits of eyeInspect extend to every organizational level, from C-level management to engineers, and span across multiple departments, from IT to OT. In fact, eyeInspect provides IT teams with guidance for an informed risk management process, real-time visibility behind the OT firewall and a continuous overview of the security status of the network. OT teams are supported in their daily activity with early detection of operational problems and threats, as well as guidance in their mitigation and resolution. The result is full control of the manufacturing environment.

The below is an overview of the major financial, strategic and technical benefits derived from the implementation of eyeInspect.

**FINANCIAL**
- Increased productivity
- Averted loss of revenue due to unplanned downtime
- Reduced costs for problem mitigation
- Easier compliance with standards and guidelines
- Minimized corporate liability
- Immediate ROI

**STRATEGIC**
- Ability to anticipate cyber incidents
- Reduced risk of downtime
- Reduced exposure to cyber threats
- Reduced resource allocation for problem identification and resolution
- Ability to perform predictive maintenance
- Evidence of good operation and accountability

**TECHNICAL**
- Full network visibility and real-time situational awareness
- Early indicators of problems and threats
- Minimized troubleshooting effort and resolution time
- Validation of network changes and maintenance operations (by employees and third parties)
- Enhanced reliability and availability of control systems

See eyeInspect in Action!
Your organization is unique. Get your demo and let us show how you can benefit from cyber resilience.

Get my Demo