NOZOMI NETWORKS

INDUSTRY BRIEF

Manufacturing: Improving Operational Resilience Through OT and IoT Visibility and Security

Table of Contents

1. Introduction 1

2. Top Manufacturing Industry Challenges 2

- 2.1 Maintaining Operational Resilience and Uptime 2
- 2.2 Employing a Cybersecurity Framework and Best Practices 3
- 2.3 Achieving Visibility Into (and Protecting) OT and IoT Networks 4
- 2.4 Integrating IT and OT Systems to Close Security Gaps 4

3. The Nozomi Networks Solution 6

- 3.1 How the Nozomi Networks Solution Improves Operational Resilience 6
- 3.2 Diagram: OT and IoT Security and Visibility 7
- 3.3 Deployment Architecture: Purdue Model Example 8

4. Improving Network and Operational Visibility 9

- 4.1 Use Case: Effectively Monitoring the ICS Network 9
- 4.2 Use Case: Keeping Production Lines Running 11

5. Detecting Cyber Risks and Improving Cyber Resilience 13

- 5.1 Use Case: Integrating IT/OT Security Efforts 13
- 5.2 Use Case: Applying Cybersecurity Best Practices 15

6. Conclusion 17

7. Customer Reviews 18

What to Look for in an OT and IoT Security and Visibility Solution 19

See the Nozomi Networks Solution in Action 19

Want to Know More? 19

8. References 20

1. Introduction

Improving Operational Resilience for Manufacturers Through OT and IoT Visibility and Security

The COVID-19 pandemic has accelerated digital transformation in the manufacturing sector. Innovation and automation are key to unlocking growth potential, but the new technologies driving digitization also increase exposure to cyber threats that can disrupt operations.

Fortunately, advanced solutions that provide real-time visibility and cybersecurity for industrial networks significantly reduce risk and build production resilience.

Small, nimble competitors entering the manufacturing space increase the pressure on established players to deliver on millennial consumer expectations. To compete, companies must deploy new technology to take advantage of interconnected systems and supply chains, artificial intelligence for predictive maintenance, and mass customization trends.

Compounding the challenge is a cybersecurity labor crisis. While automation can reduce the number of low-skilled roles and increase operational productivity, more plant floor connectivity opens the network to threats that require a new set of IT/OT (operational technology) skills.

From a cybersecurity standpoint, manufacturers have traditionally flown under the radar. Threat actors initially targeted critical infrastructure, such as energy and transportation, and industry and governmental security oversight followed.

But, according to the 2018 Cybersecurity for Manufacturing report, manufacturing is now the third most targeted industry, behind only government systems and finance.[1] And nation-state sponsored and other malicious hackers are taking full advantage of the opportunity. According to the Verizon's 2019 Data Breach Investigations Report, intentional attacks on manufacturing by outsiders accounted for 70% of all breaches reported.[2]

External threats, however, aren't the only risks that keep company leaders awake at night—accidental and unintentional cyber incidents caused by employees or suppliers can impact productivity as well. Given the large number of vulnerable devices and insecure processes, the risk of some type of breach is very real. And, despite a historic lack of industry oversight, guidelines and regulations are coming.

THE ROAD TO OPERATIONAL RESILIENCE

Read this paper to learn how a unified OT and IoT monitoring and threat detection solution can be used to **achieve operational availability, visibility and security.**

Manufacturers, including the food and beverage, chemical, pharma and automotive sectors, need to get ahead of the curve. The first step is to adopt a cybersecurity framework that IT and OT can collaborate on. Armed with cybersecurity best practices and the right technology, companies can protect their production, people and reputation, while preserving the bottom line.

2. Top Manufacturing Industry Challenges

As manufacturers automate and digitize, they face the following challenges that, if not properly addressed, leave them exposed to significant business risks.

2.1 Maintaining Operational Resilience and Uptime

Interconnectivity between enterprise and operational networks opens the door for cyberattacks. So does external connectivity spurred by Industry 4.0 and the Industrial Internet of Things (IIoT). That means that if a production line goes down, companies can lose millions within minutes.

While that's a worst-case scenario, manufacturers are hyper-aware of the potential financial impact of downtime. For this industry, maintaining 24/7 uptime is business-critical.

In 2017, for example, British consumer goods company Reckitt Benckiser Group suffered an estimated $117 million loss after a NotPetya attack. The malware caused widespread business disruption, information loss, revenue loss and equipment damage across multiple markets.[2] Dubbed by many to be the most devastating cyberattack in history, NotPetya cost Reckitt Benckiser 1% of its annual sales – and inflicted $10 billion in damages across industries globally.[3]

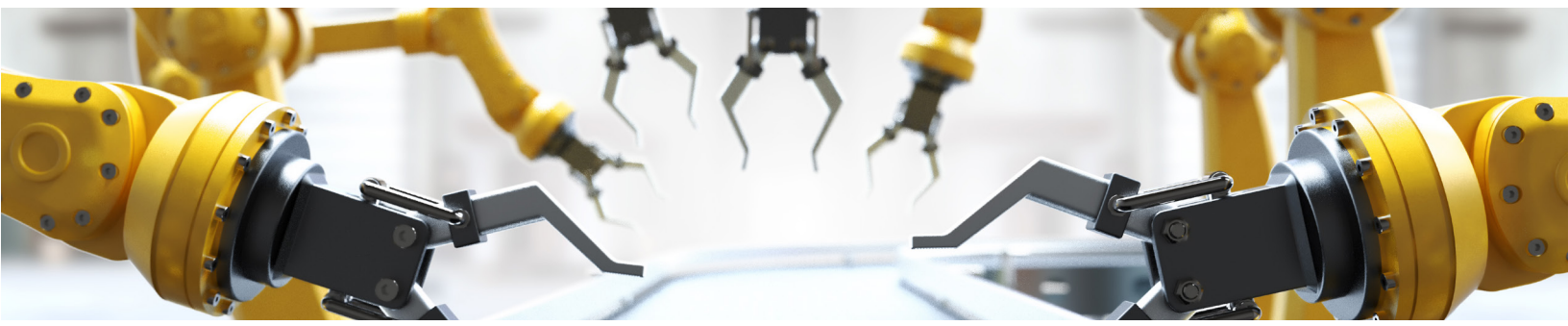
Due to the impact downtime can have on manufacturers' ability to deliver product to market, many opt to keep additional inventory on hand as a risk mitigation tactic. Producing and storing extra inventory for days or even weeks at a time is an expensive proposition. It also takes manufacturers away from just-in-time (JIT) manufacturing – an ideal inventory control method that increases productivity while lowering costs. Instead, companies have been forced to delay their inventory turnover due to fear of cyber incidents that could disrupt operations.

THE HEAVY BURDEN OF OPERATIONAL DOWNTIME

For the manufacturing industry, maintaining 24/7 uptime is business critical.

In 2017, British consumer goods company Reckitt Benckiser Group suffered an estimated $117 million loss after a NotPetya attack.

To protect production lines, manufacturers can take advantage of OT risk detection and mitigation solutions that don't compromise uptime.



2.2 Employing a Cybersecurity Framework and Best Practices

Devastating and costly cyberattacks dominate the news media, leaving manufacturers to consider, "What would happen if an attack hit our organization?" From NotPetya to WannaCry[4] to Dragonfly 2,[5] these malware attacks wreak havoc on manufacturers' ability to operate, and ultimately cause massive financial hits to the bottom line.

As companies look at their security posture and practices, executive leadership and Boards of Directors fear that while IT functions appear to be well covered, no visibility or protection is in place for operations. OT teams are feeling the pressure from the CIO, or Chief Information Security Officer (CISO), to ensure that company IP, technology and production processes are adequately protected.

And while the manufacturing sector has largely flown under the radar, cyber regulations are now being developed for nearly every industrial sector. Getting ahead of the curve before government mandates come down has manufacturers working fast to determine the steps needed to improve cyber resilience—or possibly even where to begin.

Top manufacturers are researching and selecting a cybersecurity framework to follow, such as IEC 62443, NIST, or NIS. These frameworks offer guidelines for cybersecurity best practices and tools for facilitating their implementation.

BEING PROACTIVE IS BEST PRACTICE

While the manufacturing sector has largely flown under the radar,

cyber regulations are now being developed for nearly every industrial sector.

With a trusted framework selected, manufacturers can identify the right people, processes and tools required for robust cybersecurity hygiene. From an accurate asset inventory to identifying potential threats, manufacturers can follow industry guidelines and best practices to attain next-level cybersecurity resilience.

2.3 Achieving Visibility Into (and Protecting) OT and IoT Networks

For decades, automation manufacturers defined their own proprietary networking protocols. In recent years, however, the industry has come to appreciate the benefits of common networking platforms to ensure compatibility across devices and properly protect their systems.

ELIMINATE NETWORK BLIND SPOTS

To transform the system architecture and achieve the required visibility, manufacturers need to employ the latest technology and best practices.

This starts with inventorying all assets on the network.

As the industry transitions, navigating a blend of new and old infrastructure can prove challenging. Between legacy OT systems and new IIoT devices being added without documentation, many teams don't have an accurate view of what's on their network. It's not uncommon for manufacturers to think that they have 5,000 devices, when the number is more like 10,000. This lack of visibility makes it nearly impossible to secure and monitor industrial networks, leaving many manufacturers unsure of where to start.

To transform the system architecture and achieve the required visibility, manufacturers need to employ the latest technology and best practices. This starts with inventorying all assets on the network. If the IT/OT team doesn't know what they have, they can't protect their assets or segment the network for better resilience.

Visibility also enables operational efficiencies and potential cost savings. For example, an inefficient network link with unusually high bandwidth usage can be easily identified. And once the full network is visible, it can be monitored on an ongoing basis for deviations. Manufacturers can then easily spot vulnerable areas and assets in need of protection – and oversee an efficient, resilient system.

2.4 Integrating IT and OT Systems to Close Security Gaps

Manufacturing executives are putting pressure on their CISOs and Operational VPs to 1) protect the company from risk and 2) transform plant operations by improving operational effectiveness. This transformation can only be accomplished with IT and OT working together.

With divergent priorities, bringing OT and IT teams and systems together can feel like an uphill battle. And as more systems converge, the vulnerability points and potential risks only continue to increase. Teams need to balance their dueling priorities and tap into each other's unique expertise.

IT can advise on cybersecurity issues and processes. OT keeps production systems running and prevents downtime. Together, these functions make holistic threat monitoring and secure data flows possible, to reduce blind spots and minimize security risks.

THE VALUE OF IT/OT COLLABORATION

The insights derived from IT/OT convergence

can optimize factory operations, enhance equipment utilization, enable predictive maintenance, and improve cybersecurity.

The insights derived from IT/OT convergence can optimize factory operations, enhance equipment utilization, enable predictive maintenance, and improve cybersecurity. And the impact doesn't end there. These insights create a more scalable system, ready to tackle new logistical challenges.

In fact, a factory's path to digital transformation reaches across the entire value chain, from product development to distribution (and beyond). With comprehensive, real-time operational visibility, plants can increase productivity and close security gaps.

3. The Nozomi Networks Solution

3.1 How the Nozomi Networks Solution Improves Operational Resilience

Nozomi Networks helps manufacturers accelerate the pace of digital transformation by unifying visibility and threat detection across OT, IoT, IT and cyber-physical systems.

We make it possible for your organization to tackle escalating cyber risks to operational networks while modernizing your business to succeed in the future.

SECURING GLOBAL MANUFACTURING LEADERS

Nozomi Networks delivers OT and IoT visibility and security to the largest manufacturing and other OT sites around the world. Through the innovative use of artificial intelligence (AI), our solution automates the hard work of inventorying, visualizing and monitoring industrial control networks.

Manufacturers benefit from the real-time visibility and threat detection needed to ensure high cyber resilience and reliability.

Following is a short description of our product line, for complete information, visit **our website**.

SAAS

Vantage

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

EDGE OR PUBLIC CLOUD

Central Management Console

The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across your distributed sites, at the edge or in the public cloud. It integrates with your IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

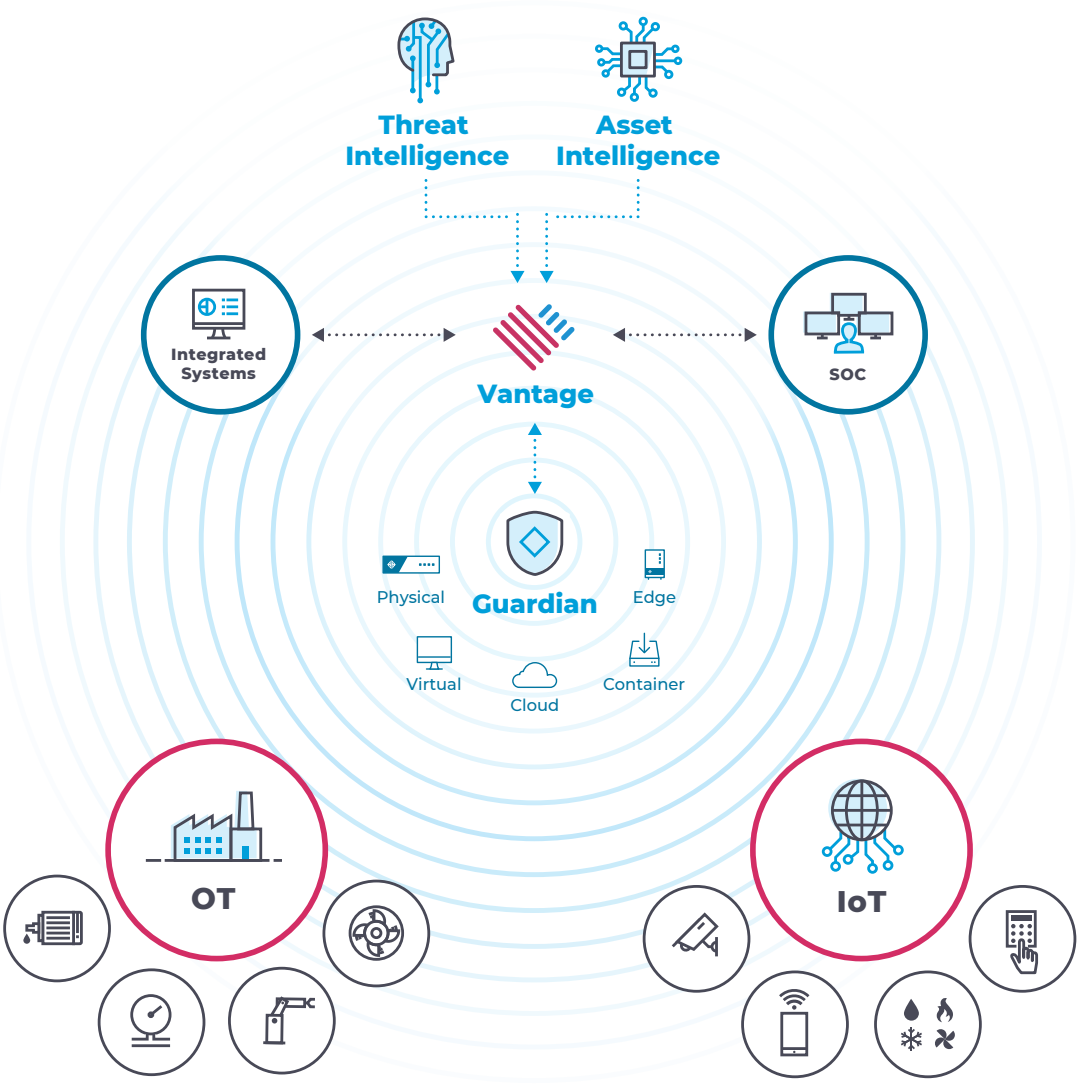
SUBSCRIPTION

Asset Intelligence

The Asset Intelligence service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

3.2 Diagram: OT and IoT Security and Visibility

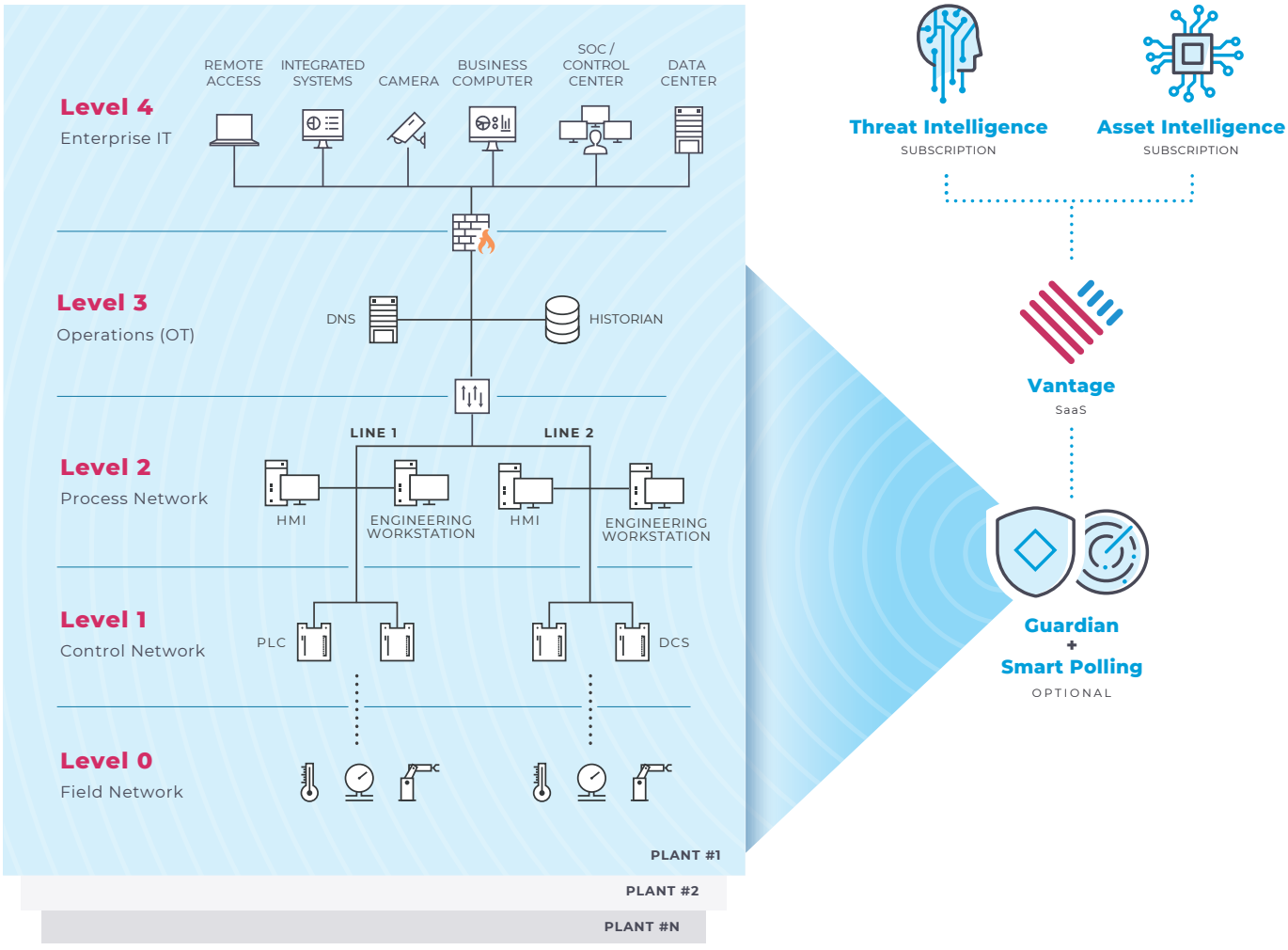
You can protect a wide variety of mixed environments with rapid asset discovery, real-time network visualization and up-to-date threat intelligence.



3.3 Deployment Architecture: Purdue Model Example

You can tailor the Nozomi Networks solution to meet your needs by utilizing its flexible architecture and integrations with other systems.

Additionally, **Remote Collectors**™ can be added to Guardian sensors to capture data from remote and offsite locations.



4. Improving Network and Operational Visibility

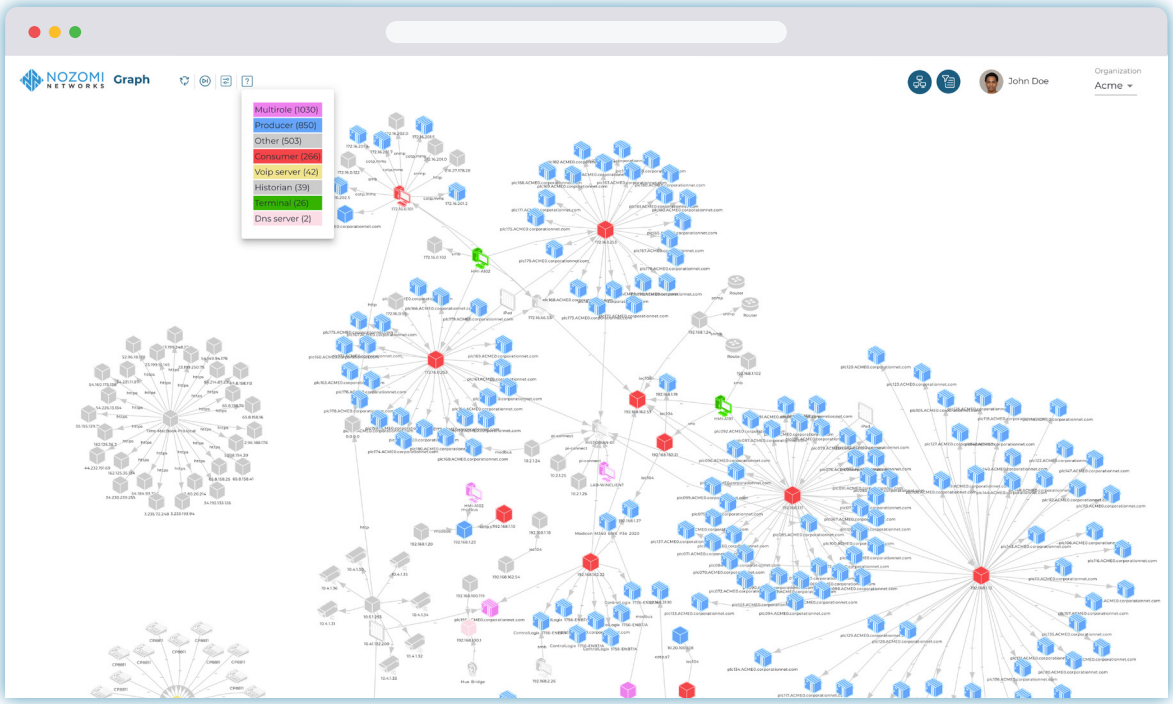
4.1 Use Case: Effectively Monitoring the ICS Network

In the world of manufacturing, one small change or networking issue can have a significant effect – on product quality, production uptime and even plant safety. Staying on top of what's happening in the industrial control network, and responding to changes fast, is mission critical.

But industrial operators can't monitor and manage what isn't visible and documented. For example, during a recent Proof of Concept, a manufacturing company stated that they had 3,000 devices on their network. When the Nozomi Networks solution was deployed, 15,000 appeared! And while working with a wholesaler, the solution uncovered devices that were thought to be decommissioned, former contractors who still had system access, and other surprising insights.

Do you really know what types of devices are on your network, and how many there are? Which ones are actively communicating and what protocols they're using? Would you know if someone intentionally or accidentally changed the configuration on a PLC, or deleted a log file?

To spot and troubleshoot networking and communication issues that threaten reliability, you need real-time visibility into your assets, connections, communications, protocols and more.



Nozomi Networks Solution: Network Graph View
This visualization displays all assets on your network for real-time awareness.

THE CHALLENGE

- Staying on top of network status and changes.

THE SOLUTION

Using real-time OT and IoT visibility to improve situational awareness.

- The Nozomi Networks solution analyzes network traffic, using the data to build a live, interactive visualization of the system, often revealing unknown aspects of OT and IoT systems.
- Manufacturers can efficiently monitor industrial networks and easily troubleshoot problems before they impact operations.

RESULTS

Network-wide situational awareness

Faster troubleshooting of system changes and issues

Better oversight of vulnerabilities and risks

Higher operational reliability

4.2 Use Case: Keeping Production Lines Running

Unplanned downtime happens for multiple reasons — a component breaks down from operating 24/7, a networking change impacts production lines, or a cyber incident disrupts communication.

Not only does it take time to understand and address the problem, valuable production capacity is lost. To mitigate risks like this, some manufacturers carry extra inventory just to cover potential downtime.

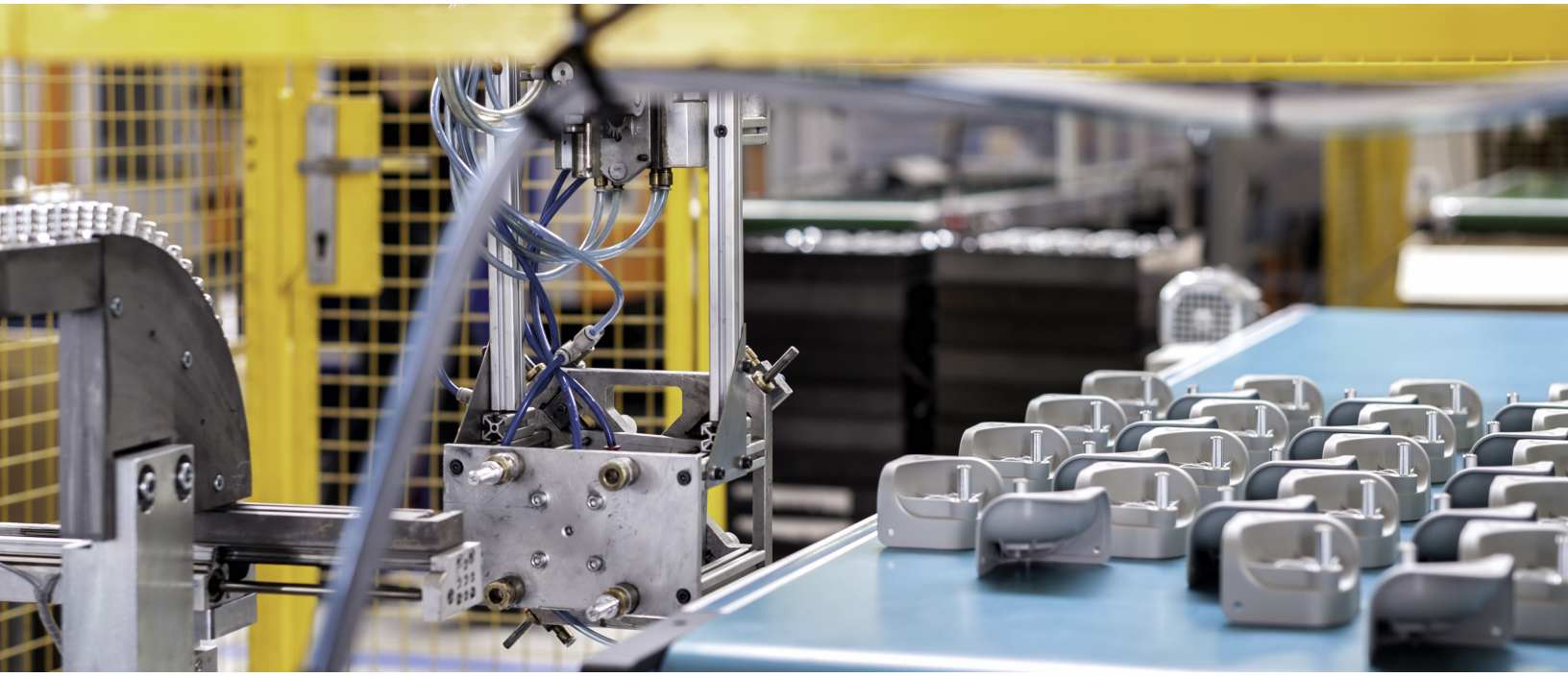
But in the manufacturing business, time is money, so planned and unplanned downtime, and excess inventory, can hit the bottom line hard. According to Gartner, the cost of downtime clocks in at somewhere between $300k–500k an hour.[6]

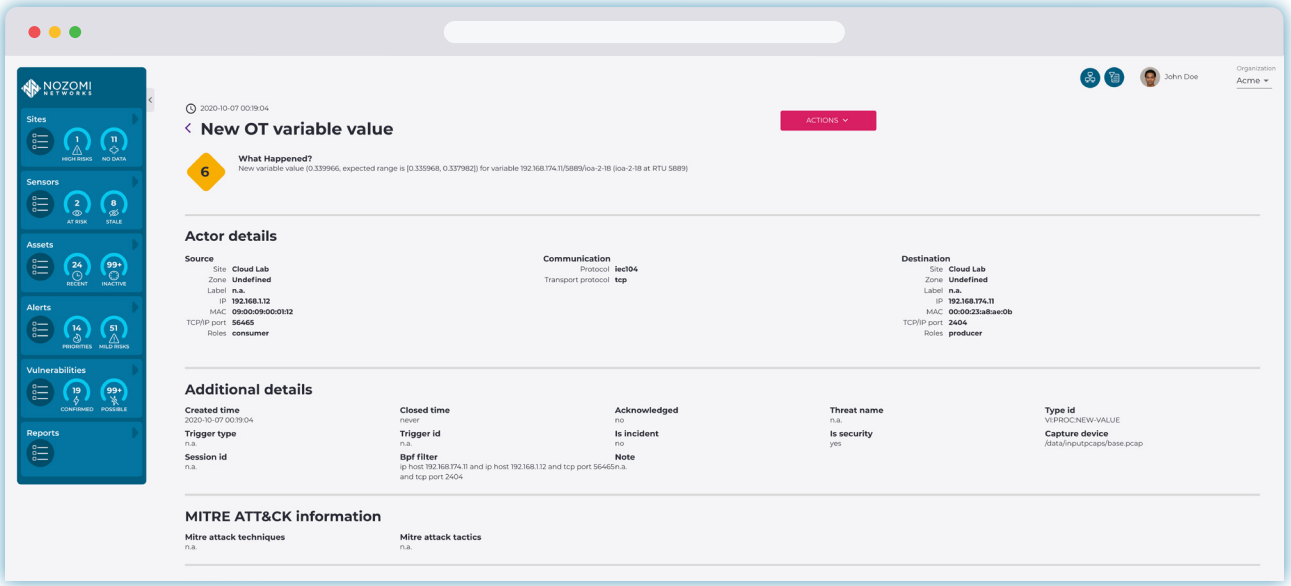
Let's take a look at the impact of downtime:

In 2019, a multinational manufacturer headquartered in Norway – one of the world's largest aluminum producers – reported that it was hit by a ransomware that affected its production and IT systems. The Extruded Solutions unit, which makes components for car manufacturing, construction and other industries, reduced its output by 50%.

Administrative systems, such as reporting, billing and invoicing, suffered delays. It took the manufacturing company several weeks to bring operations back to normal. Lost margins and low production volumes were estimated to cost up to $70 million.[7]

Can you imagine the benefits of proactively identifying potential equipment problems, cyber threats, and bringing your stock on hand down by 50% or more?





Nozomi Networks Solution: OT Variable Alert
Unusual device or system behavior could lead to operational disruption and serious safety incidents.

THE CHALLENGE

- Preventing loss of production capacity.

THE SOLUTION

Using Anomaly Detection to Identify At-Risk Devices and Processes Before They Fail

- The Nozomi Networks solution protects against operational disruption by detecting when a specific device or automated operation is deviating from its baseline and moving towards a state that could disrupt services. It also identifies if vendor work has been completed or not, ensuring that maintenance is done on time.
- Operators leverage a simple, consolidated view of what's happening and receive alerts prompting them to act before a device or automated operation fails.

RESULTS

Proactive detection of potential equipment failure

Reduced troubleshooting and forensics

Faster problem resolution

Maximized production line uptime

5. Detecting Cyber Risks and Improving Cyber Resilience

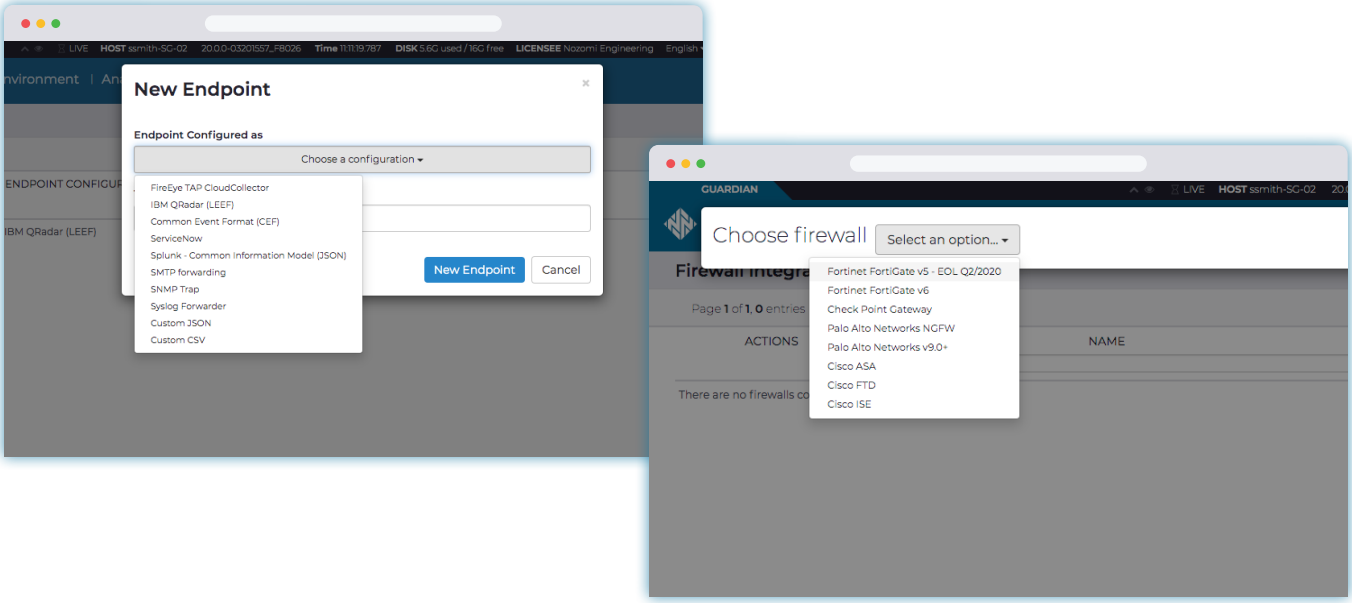
5.1 Use Case: Integrating IT/OT Security Efforts

OT knows how to meet production targets and keep the plant running. IT has the expertise to address networking and cybersecurity issues that are unfamiliar to ICS staff. Wouldn't it be great if the OT and IT teams worked together to build operational resilience?

Unfortunately, oversight of OT security can be quite fragmented. A report by Automation World found that less than 8% of companies surveyed had combined the two departments, while 24% saw almost no interaction between them.[8]

Sometimes OT security is managed by the engineering technology group, in other cases by a plant manager. Sometimes, an IT team member has moved across to OT to handle it, other times, there is little to no interaction between IT and OT.

Yet collaboration between IT and OT is critical to reducing the blind spots and security risks surrounding highly connected industrial control systems. As "smart" factories leverage more IIoT technology, and OT networks become more connected to business networks and the cloud, the IT/OT divide puts business at risk.



Nozomi Networks Solution: Easy IT/OT Integration
Built-in support for many asset and identity management systems, firewalls, SIEMs and more makes it easy to integrate and share OT and IoT system information across IT/OT environments.

THE CHALLENGE

- Leveraging IT expertise with OT production know-how to improve resilience

THE SOLUTION

Aligning IT and OT with a single solution.

- The Nozomi Networks no-risk solution provides IT and OT with deep visibility into ICS assets and continuous monitoring for risks that could impact reliability or cybersecurity. It provides a common platform to drive IT/OT convergence.
- Manufacturers can easily integrate real-time OT monitoring into overall security infrastructure for improved operational resilience and reliability.

RESULTS

Reduction of OT security blind spots

Continuous monitoring for better oversight of threats, violations and risks

Faster troubleshooting

OT threat monitoring that is fully integrated into the overall security mandate

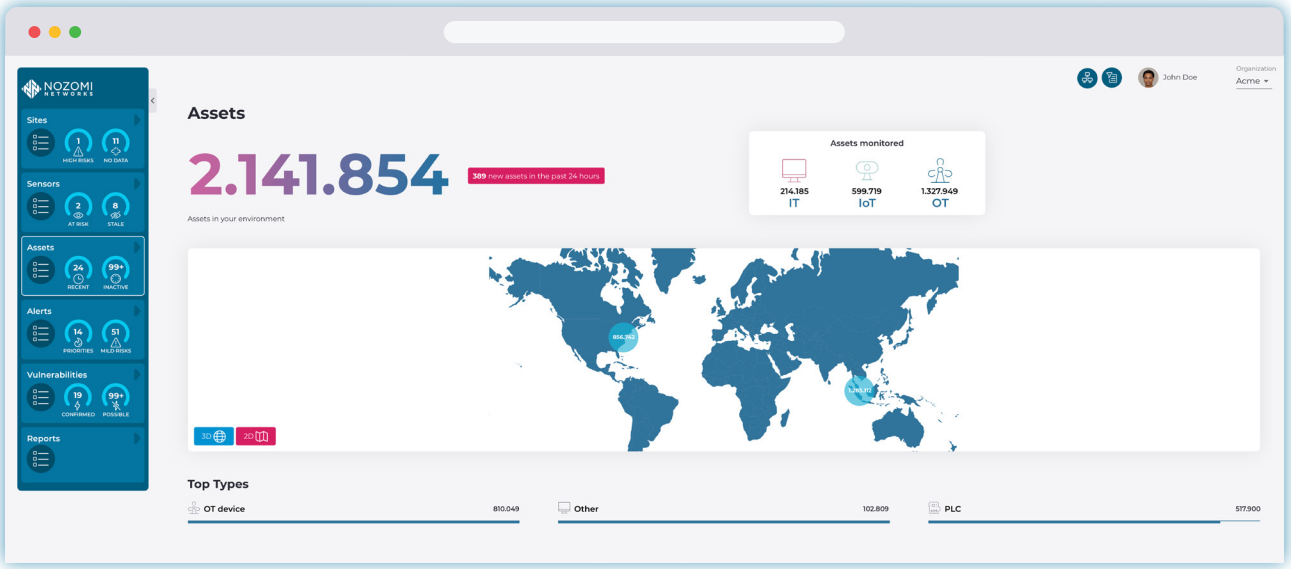
5.2 Use Case: Applying Cybersecurity Best Practices

Operational risk comes from multiple sources, including people, processes and technology. According to the Verizon 2019 Data Breach Investigations Report, intentional attacks on manufacturing by outsiders accounted for 70% of all breaches reported.[2]

But while malware and other high profile cyberattacks get a lot attention, the SANS Institute reports that 28% of ICS professionals rank insider (and often accidental) incidents as a top threat vector. The organization's recently released OT/ICS Cybersecurity Survey found that 62% of respondents rated "people" as the riskiest pillar for compromise, well behind technology and processes.[9]

Examples of human-generated operational risk include device configuration errors, open ports, the use of weak passwords, and forgetting to remove a contractor's access after they've left the organization.

Given the significant risk to operations, it's not surprising that OT leaders want to up their security game. But how do you implement a cybersecurity framework, and take cyber resilience to the next level?



The Nozomi Networks Solution: Assets View
This view summarizes the asset status across facilities for real-time situational awareness and risk assessment.

THE CHALLENGE

- Building organization-wide security maturity

THE SOLUTION

Using anomaly detection to identify at-risk equipment before it fails.

- The Nozomi Networks solution makes it easy to understand and adopt cybersecurity best practices, such as those outlined by the NIST Cybersecurity Framework Manufacturing Profile, IEC 62443 and ISO 27000.

  For example, NIST outlines five security framework functions – identify, protect, detect, respond and recover, that should be incorporated into your operational processes to address cyber risk. Identification includes asset management and risk assessment, while detection includes continuous monitoring and insight into anomalies and events, among other functions.
- With the adoption of an OT visibility solution, manufacturers can automate the creation of an asset inventory, and continuously monitor their network and ICS. They can also rapidly identify vulnerabilities and proactively identify threats to the security of their industrial control systems.

RESULTS

Adoption of cybersecurity frameworks and best practices

Proactive identification and mitigation of operational risks

Improved operational resilience

6. Conclusion

Operational Visibility and Cybersecurity Boost Manufacturing Resilience

Manufacturers are embracing digital transformation to find efficiencies and grow revenue. In doing so, they'll inevitably need to address common operational challenges – such as gaining visibility into their OT and IoT networks and closing security gaps.

SECURING GLOBAL MANUFACTURING LEADERS

Without OT and IoT visibility, it's difficult to stay on top of what's happening on the network. One small change or networking issue can impact product quality, production uptime, plant safety, and revenue.

Spotting and troubleshooting issues that threaten reliability requires real-time visibility. Unfortunately, many manufacturers lack insight into their devices, connections, and communications.

Security gaps related to people, processes and technology can have a big impact on operational resilience too. For example, the separation of IT and OT, combined with increasingly connected industrial control systems, can lead to cybersecurity blind spots. But with the right technology and a focus on best practices, manufacturers can improve their operational resilience.

With the Nozomi Networks solution, visibility and cybersecurity are easy to achieve. It delivers improved OT and IoT visibility by automatically creating an up-to-date inventory of all assets on the network. It then monitors their behavior for anomalies and alerts operators to changes that could indicate potential problems. The solution also provides advanced vulnerability and threat detection, along with detailed insights that lead to faster prioritization and remediation.

Tailored to meet the unique challenges of manufacturing, the Nozomi Networks solution helps operators gain deeper operational visibility, apply security best practices and align IT and OT.

It significantly helps to monitor OT/IoT networks, keep production lines running, integrate IT/OT security efforts and apply cybersecurity best practices.

FIND OUT MORE

Manufacturers can benefit greatly from investing in a network visibility, monitoring and security solution.

Find out how quickly the Nozomi Networks solution can boost operational resilience for you.

Contact us at **nozominetworks.com/contact**

7. Customer Reviews

Manufacturing Customers Give Nozomi Networks Top Score

★★★★★

Exceeded Expectations. Deeper Visibility Than Expected.

We place an emphasis that every vendor we engage with understands we are not a set up for a “cookie cutter” type of solution. I honestly expected this to be a problem for most if not all vendors. And I was correct, with Nozomi being the sole exception. Not only has their solution done as advertised, and then some.

Senior Industrial Security Manager ›

Once You Try Nozomi And Its Rich Feature Set You Cannot Imagine Operating Without It!

We put Nozomi head to head against other similar products and the Nozomi platform was able to pick out and properly categorize more L2 devices than any other tool in the market place at the time of test.

Security Analyst ›

Great Solutions For ICS.

The solution still has many features that manage the OT environment, such as inventory and vulnerability analysis capabilities. An extra point for the solution is the communication flow map of the neural network, containing information of great relevance for an incident response.

IT Analyst ›

For more reviews, visit our website.

See All Reviews

What to Look for in an OT and IoT Security and Visibility Solution

Technology advancements, such as those found in the Nozomi Networks solution, can dramatically improve security and reliability.

When choosing a solution, look for the following characteristics:

- Comprehensive visibility of all assets in your network
- Advanced threat detection
- Accurate anomaly alerts
- Proven scalability
- Easy IT/OT integration
- Global partner ecosystem
- Exceptional customer engagement and support

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

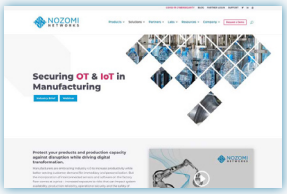
Contact Us

Want to Know More?

SOLUTION BRIEF

Nozomi Networks

DOWNLOAD



WEBPAGE

Manufacturing

VISIT

DATA SHEET

Vantage

DOWNLOAD

DATA SHEET

Threat Intelligence

DOWNLOAD

8. References

1. **"Cybersecurity for Manufacturing,"** Make UK (formerly EEF), 2019.
2. **"2019 Data Breach Investigations Report,"** 11th Edition, Verizon, 2019.
3. **"How Much Did a Cyberattack Cost Reckitt Benckiser? Try $117 Million,"** AdAge, 2017.
4. **"WannaCry: A Wake-up Call to Revisit ICS Cybersecurity Measures,"** Nozomi Networks, 2017.
5. **"Russian Cyberattacks on Critical Infrastructure – What You Need to Know,"** Nozomi Networks, 2018.
6. **"The Cost of Downtime,"** Gartner, 2014.
7. **"First Quarter 2019 Report,"** Hydro, 2019.
8. **"Bridging the IT and OT Divide,"** Automation World, 2017.
9. **"SANS 2019 State of OT/ICS Cybersecurity Survey,"** SANS, 2019.
10. **"Cybersecurity Framework Manufacturing Profile,"** NIST, 2017.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

IB-MANU-8.5x11-005

nozominetworks.com