



**NOZOMI**  
NETWORKS

# A proactive approach to Cybersecurity in OT and IoT Environments for W /W W

Sandeep Lota  
Global Field CTO



# Continuous Innovation in OT and IoT Security



First **AI-powered ICS** visibility and cybersecurity solution

**September 2013**



First to offer a powerful combination of **active + passive** asset discovery

**August 2018**



First **container-based delivery model** for embedded deployment and efficiency

**June 2019**



**Vantage** pioneers **SaaS-powered** security and visibility solution for dynamic IoT and OT networks

**October 2020**



**Threat Intelligence Feed** supports third-party platforms

**June 2022**



**Nozomi Arc** launches, turning any endpoint into a security sensor

**2023 January**

**2017 November**

First **hybrid ICS threat detection** combining behavior-based anomaly detection with rules-based detection



**2018 October**

First OT monitoring solution paired with a **Threat Intelligence service**



**2020 February**

Guardian is the first product with highly accurate **IoT network anomaly detection** and **Asset Intelligence service**



**2022 March**

Nozomi Networks offers **Content Packs** as a vehicle to share queries and dashboards with the community at large for a common threat or shared process



**2022 November**

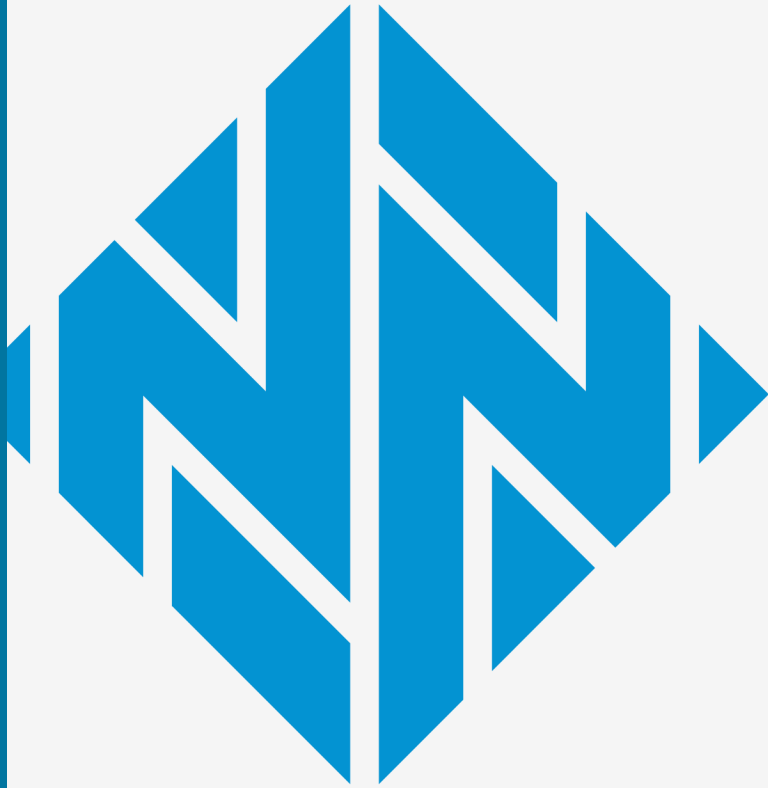
Nozomi Networks introduces **OnePass**, a single subscription to both hardware and software



**2023 May**

**Vantage IQ** announced, an industry-first AI rules-based analysis and query engine





# #1 for the 3rd Year in a Row: Gartner Peer Insights Operational Technology Security

[Learn more](#) →

**102M+**

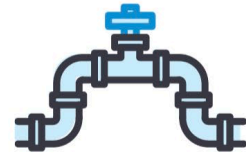
OT, IoT and IT  
Devices  
Monitored

**11K+**

Installations  
Worldwide

**100%**

Customer  
Retention



**Water utilities face serious cybersecurity threats, but often struggle with a lack of resources to ensure a strong cybersecurity program. We help water and wastewater utilities maintain resilience and do more with less.**

Los Angeles Times

May 8<sup>th</sup>, 2023

CALIFORNIA

Cracks, hacks, attacks: California's vulnerable water system faces many threats

## 50,000 security disasters waiting to happen: The problem of America's water supplies

"If you could imagine a community connected to an average water plant," one cybersecurity expert said.

INDUSTRIAL  
CYBERSECURITY PULSE

## Throwback Attack: Kemuri Water Company attack puts critical infrastructure at risk

GARY COHEN FEBRUARY 3, 2022



The only reason why Cyberattacks on Water Companies OT environments hasn't been more catastrophic is:

The attackers didn't know what they were doing...

# *A changing world requires innovative AND proactive solutions*



- Air gapped environments are no longer secure
- Increased complexity of cyberattacks pose an unprecedented challenge for OT environments
- Artificial intelligence, the ultimate tool at the hacker's fingertips
- Aging infrastructure and unsupported software is a tremendous liability

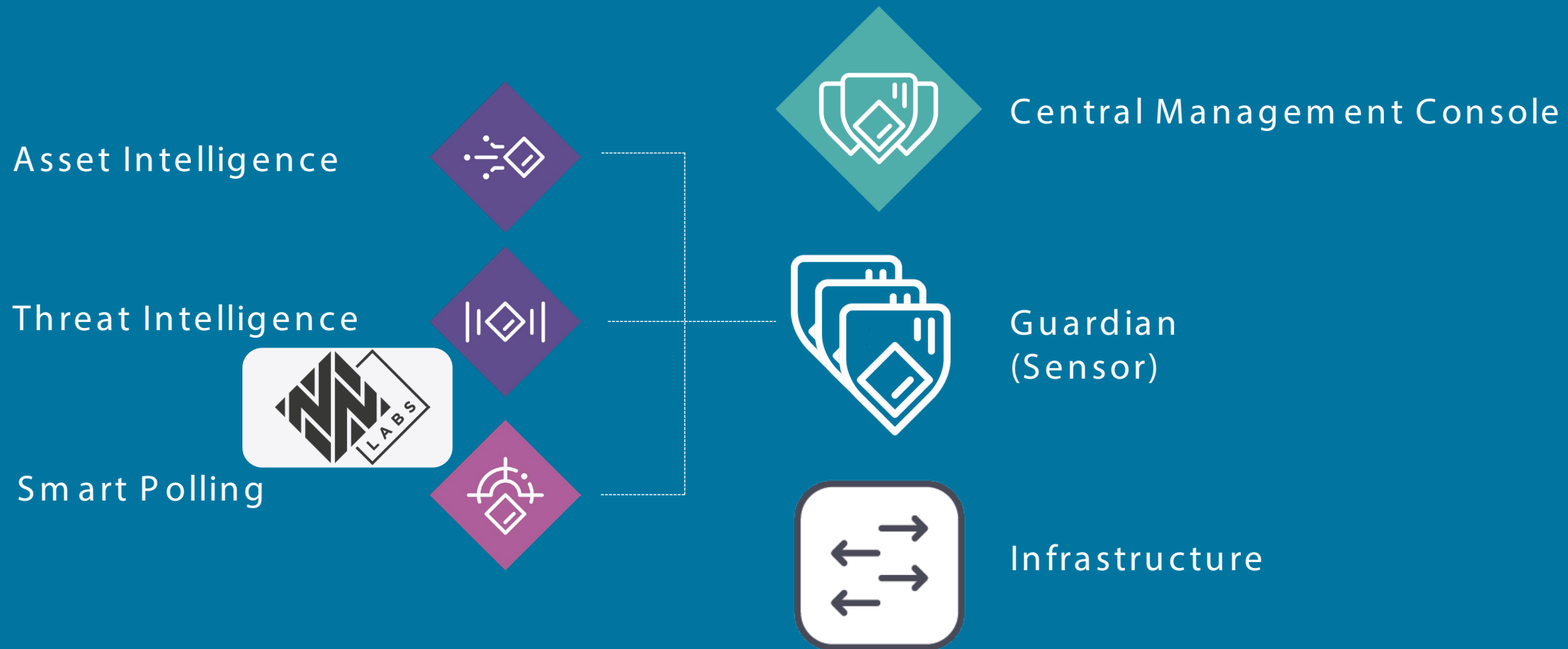


# What now?



# The Nozomi Networks approach

Completely on-prem based solutions

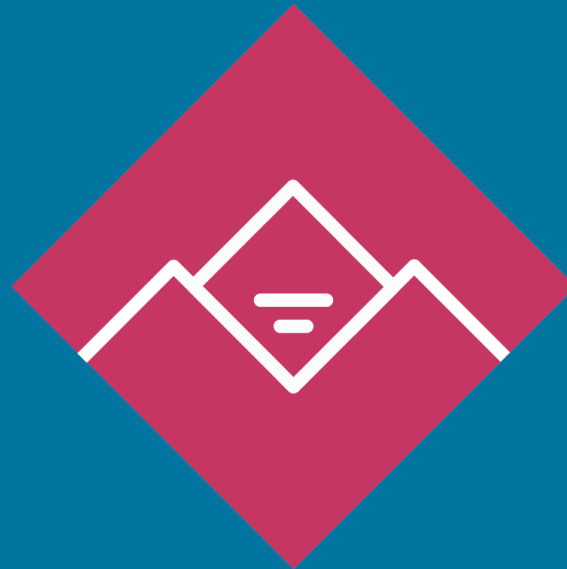


# The Nozomi Networks approach

Optional SaaS integrations and management



Vantage



Vantage: The power of cloud, for increased scalability, processing power and faster detection.

Vantage IQ: AI-assisted data analysis that helps security teams reduce cyber risk, speed response.

Vantage IQ

# Benefits of Our Cybersecurity Solution for Water & Wastewater



**Identify and manage every operational technology asset**



**Prioritize cyber risks and vulnerabilities faster**



**AI-powered threat detection and analysis to help your teams do more with less**



**Exceed regional regulatory requirements**



“I’m not comfortable connecting to the cloud”

In the past you could afford not to be connected to the cloud.

Today, being isolated represents a greater risk.



# The Nozomi Networks approach

Cybersecurity in OT and IoT, from reactive to proactive

Vantage / IQ

CMC

Guardian

Arc / RC



A complete solution designed for OT and IoT that helps mitigate internal threats, with added value.



# “I Have Firewalls”

Chances are: Your firewalls are not designed for your OT/IoT environment. Let the experts do what they are experts at.

# OT Attack vectors

## The Network

Breach the network first, to gain access to lower levels of the OT environment.

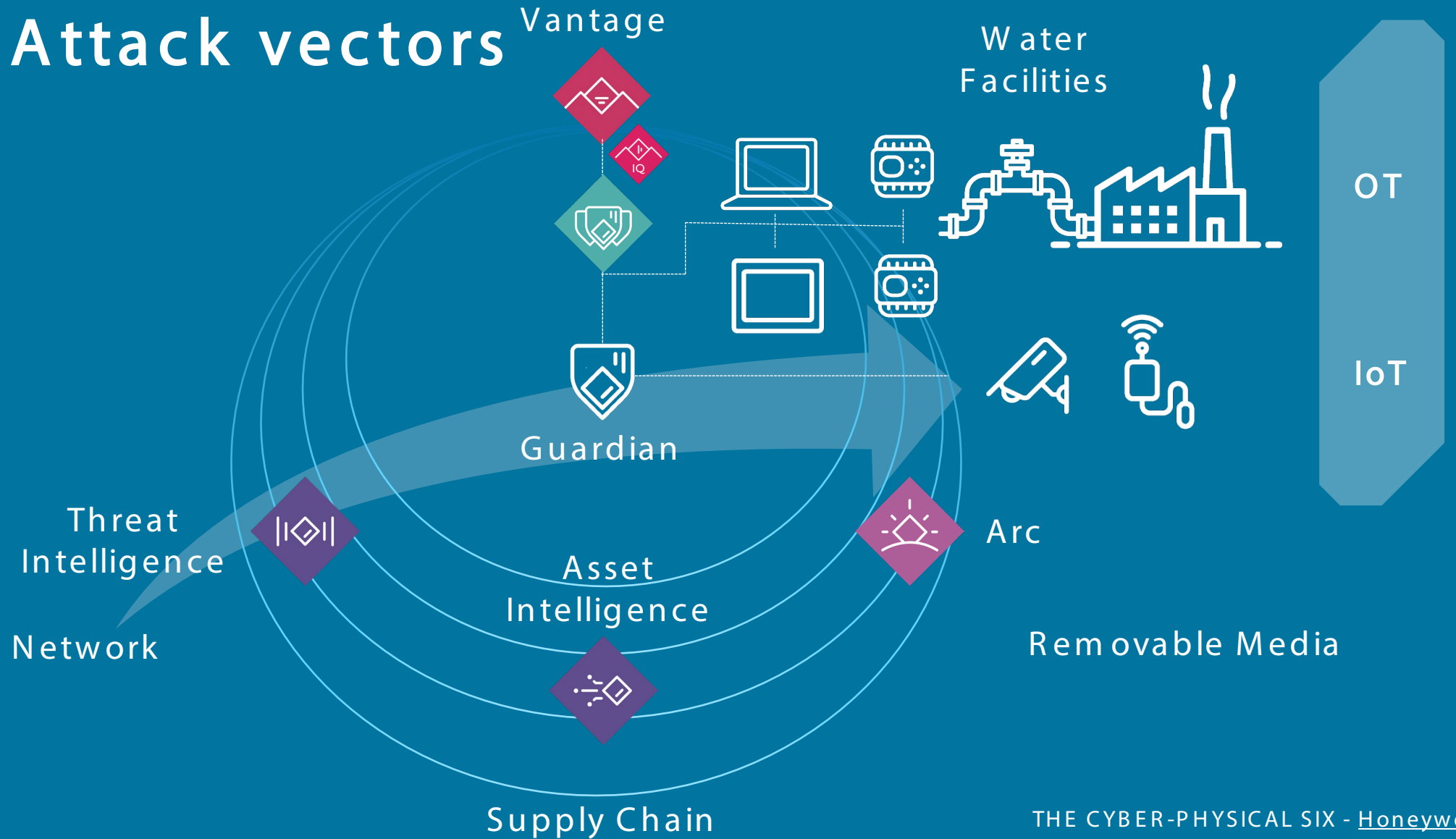
## Removable Media

Attacks using removable media, like USB thumb drives, can bypass the network security protocols.

## Supply Chain

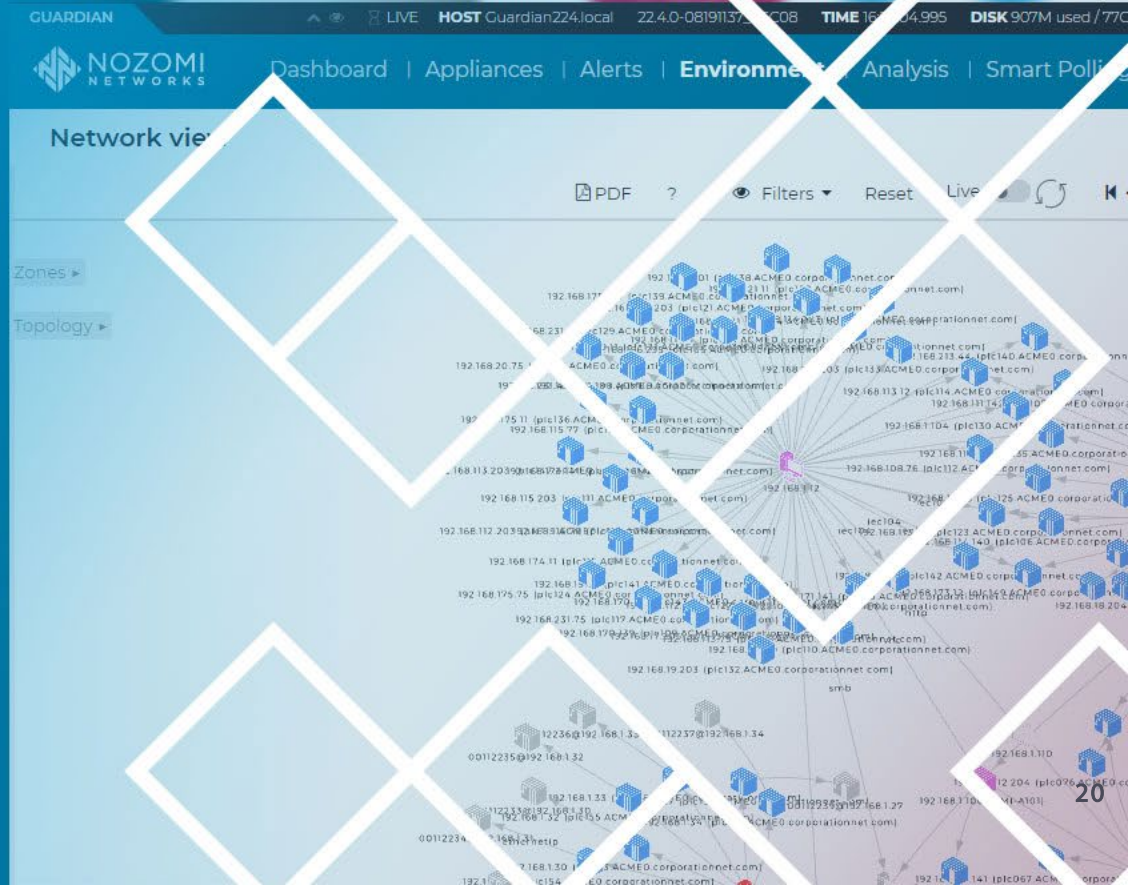
Maliciously modified hardware can be used to gain access to the infrastructure.

# IoT/OT Attack vectors





Don't be a  
statistic, act now



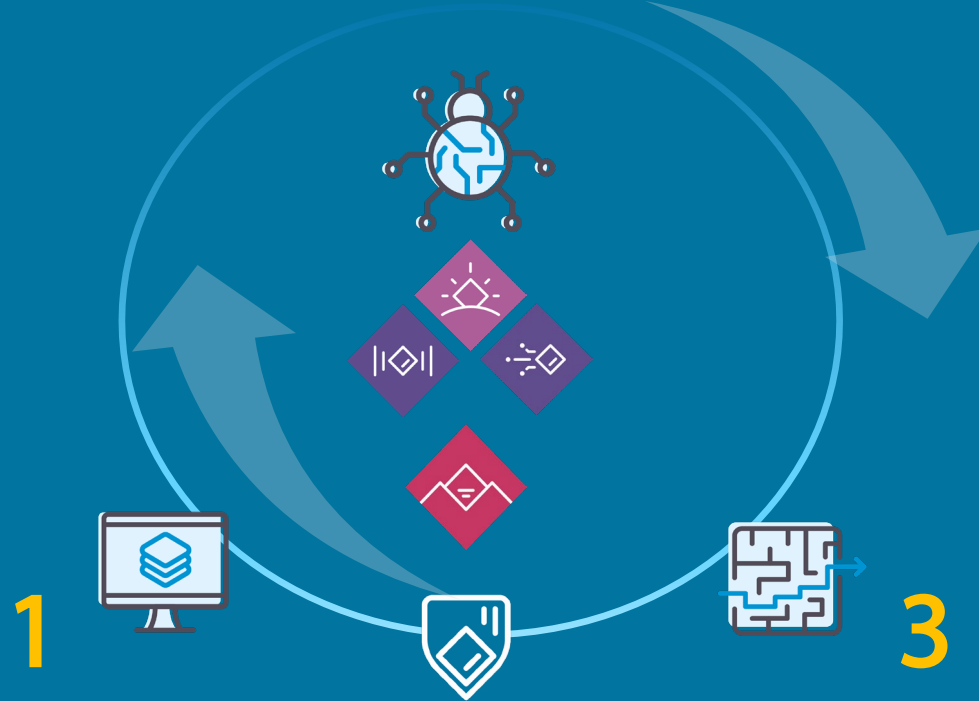
We enable  
you to:



2  
Detect

1  
Visualize

3  
Respond



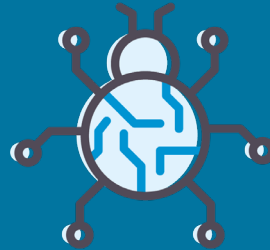


## Visualize



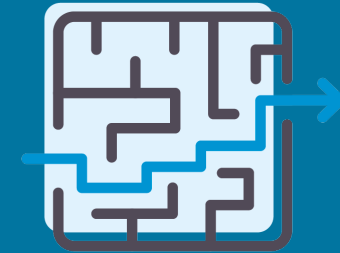
- Network and endpoint Monitoring
- Alert management
- Time Machine Function
- Query system

## Detect




- Advanced Threat Detection
- Asset Intelligence
- Enhanced Communication

## Respond



- Asset identification
- Correlation
- Integrations

A proactive approach to Cybersecurity in OT and IOT Environments



You can't  
measure ROI  
when what you  
get in return is  
measured in  
saved lives

# Where Are You Starting Your Cyber Resilience Journey?

## Asset Inventory Management

Discover every connected asset in your ICS networks.

[Learn More →](#)

## Threat Detection & Response

Detect and prioritize anomalies with AI-powered analysis.

[Learn More →](#)

## Continuous Operational Monitoring

Detect process anomalies, failing equipment and network misconfigurations to prevent downtime.

[Learn More →](#)

## Complying with Regional Regulations

Prepare with continuous monitoring that exceeds government guidelines.

[Learn More →](#)



Thank you

*"If you don't like change, you will like  
irrelevance even less"*

Gen. Eric Shinseki