NOZOMI NETWORKS

GUIDE

Buyer's Guide to OT & IoT Asset Inventory Solutions for Security Leaders

Pick your framework — asset visibility is the foundation of operational technology (OT) and Internet of Things (IoT) cybersecurity. Whether you're aligning with IEC 62443, NIST Cybersecurity Framework 2.0 or the SANS Five Critical Controls for ICS, asset inventory is where you start. Why? Because you can't manage what you can't see.

Before you can assess risk, segment your network, manage vulnerabilities and implement effective incident response plans, you must know what's on your network and what it's communicating with.

For something so fundamental, there's wide variation in what vendors mean by asset inventory management. If you cut corners at this fundamental step, instead of an actionable foundation for your cybersecurity program, you may end up with a glorified database of IP addresses.

Read this guide to learn more about:

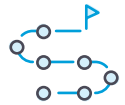
Key challenges to achieving a complete, accurate OT/IoT asset inventory

The **five pillars** to look for in an industrial asset inventory security solution

Top questions to ask when evaluating asset inventory solutions

Table of Contents

Key Challenges to Achieving a Complete, Accurate OT/IoT Asset inventory



Digital transformation over the last decade has increased the complexity of industrial asset inventory. To increase efficiency, today's environments have an explosion of assets and asset types that radically expand the attack surface and introduce new challenges.

Lack of Visibility

With no centralized view of assets across OT, IoT and IT environments, blind spots expose you to risk.

Diverse Environments

Wide variety of vendors, protocols, and device types (PLCs, RTUs, sensors, HMIs, etc.).

Legacy Tools & Infrastructure

Older equipment may not support modern monitoring or discovery tools. Firmware and OS versions may be outdated or un-patchable.

Discovery Limitations

Balancing active and passive discovery methods to identify all devices without disrupting operations.

Security Risk & Compliance

Difficulty complying with standards like NIST CSF 2.0, IEC 62443 or NERC CIP without accurate asset data and context.

Dynamic Environments

Frequent changes in the environment (e.g., contractors adding new devices, mobile assets) lead to inventory drift.

Siloed Teams & Tools

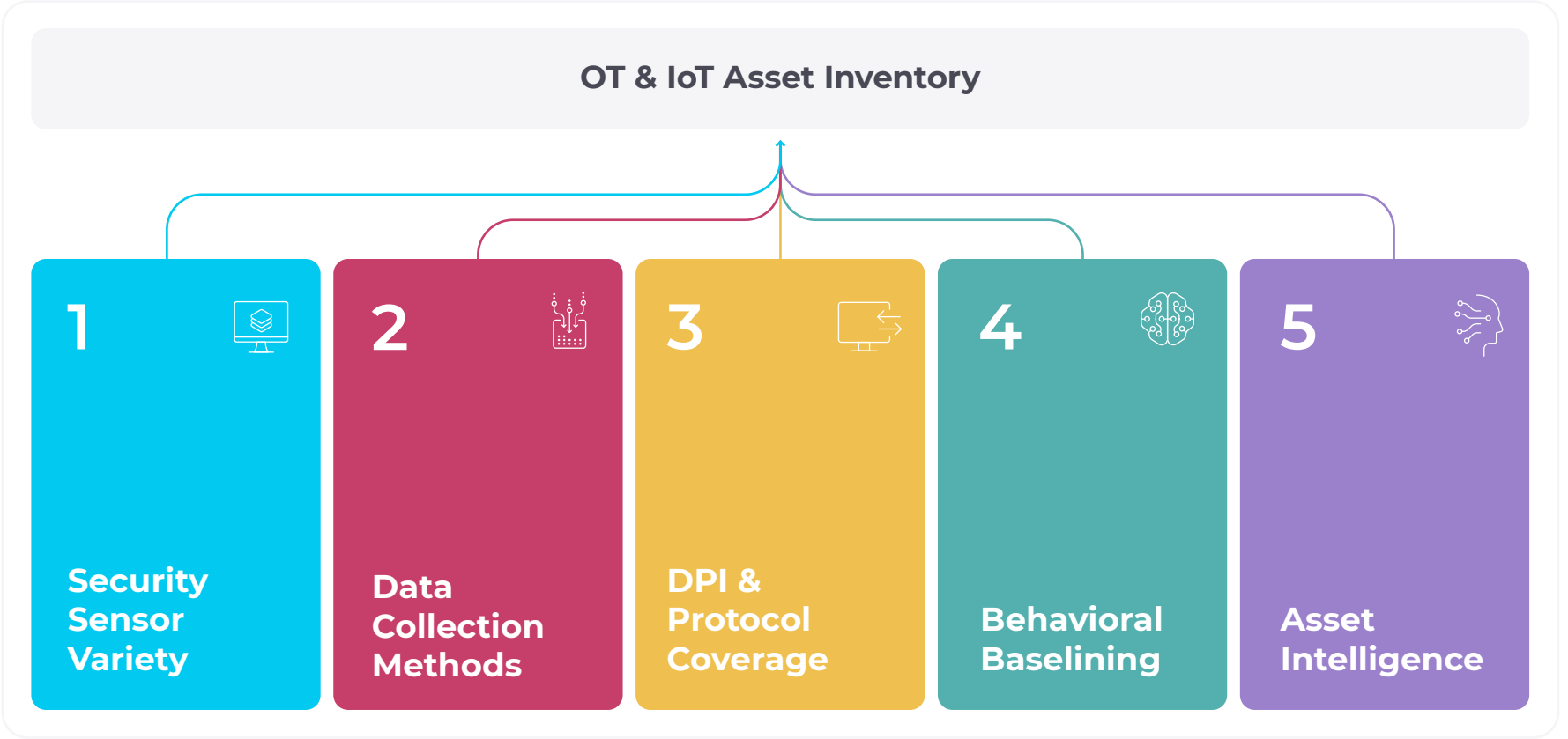
IT teams often use different tools, have limited understanding of industrial environments and may not collaborate effectively.

Incomplete Context

Asset tools may not provide operational context such as firmware version, communication patterns or process relevance.

5 Pillars to Look for in an OT & IoT Asset Inventory Solution

To serve as the foundation of your cybersecurity program, an asset inventory solution must do much more than discover and identify assets. It must also provide deep insights into device behavior and communications. Here are the five pillars to evaluate.



1. Security Sensor Variety

Discovering and identifying every asset in your environment requires a variety of sensors beyond traditional network sensors. Each of these sensor types must be purpose-built for OT/ICS environments to read industrial protocols and be non-disruptive.

Network sensors and remote collectors

Network sensors and remote collectors passively collect, analyze and visualize network data for continuous monitoring and threat and anomaly detection. Guardian network sensors observe local traffic without agents or interrogation to identify devices and monitor activity. Form factors include rack-mounted hardware, ruggedized hardware, virtual, portable and containerized.

Small, low-resource remote collectors work with Guardian sensors to capture data from hard-to-reach or unmanned locations such as wilderness, offshore and distributed locations where network sensors aren't cost efficient or practical.

Wireless sensors

The explosion of wireless connected devices in industrial and critical infrastructure environments has vastly increased the attack surface. In addition to Wi-Fi and Bluetooth, process control networks rely on specialized wireless protocols designed to facilitate reliable communication between sensors and controllers with low power consumption. Nozomi Guardian Air is the first wireless

Nozomi Networks offers the industry's most complete sensor portfolio with network, wireless and endpoint sensors.

NETWORKS SENSORS

GUARDIAN

ANSSI-CERTIFIED | FIPS COMPLIANT

REMOTE COLLECTOR

WIRELESS SENSORS

GUARDIAN AIR

ENDPOINT PROTECTION SENSORS

ARC

ARC EMBEDDED

sensor designed to detect not just Wi-Fi and Bluetooth but Zigbee, LoRaWAN, Drone RF and other wireless protocols frequently used in OT/IoT environments.

Endpoint sensors

In IT security, endpoint agents are ubiquitous for anti-virus protection and patching. Unfortunately, negative experiences deploying IT-focused agents on OT devices have led to scarce adoption of much-needed endpoint monitoring in industrial environments. That's equally risky.

Traditional ICS network monitoring solutions monitor North-South traffic between Purdue levels or firewalls, but East-West communications between devices within a zone, especially at lower Purdue levels, have long been a blind spot. Moreover, endpoint monitoring is the only way to correlate user activity and events to detect insider threats.

Nozomi Arc is a lightweight, non-disruptive security agent for Windows, Linux and MacOS that understands OT/IoT protocols and doesn't operate at the kernel level of the host operating system.

Endpoint embedded sensors

Visibility into east-west traffic at Purdue Levels 1 and 0 is typically a black hole, including industrial controllers and their backplane communications. Yet any disruption at Purdue lower levels could directly impact production.

The first version of Arc Embedded, developed in collaboration with Mitsubishi Electric, is available for the MELSEC iQ-R family of PLCs, with more OEM devices in development. Arc Embedded provides unprecedented visibility into controllers and the field assets they control, all the way down to Purdue Level 0.

2. Data Collection Methods

The second thing to look for in an industrial asset inventory solution is a variety of data collection techniques. Relying on passive discovery alone isn't enough to keep up with the increasing sophistication and frequency of industrial threats. You need a mix of passive and active discovery techniques, combined with the ability to integrate data stored in other parts of your security stack.

Passive discovery

Passive discovery through network sensors has long been the standard for OT/ICS asset discovery where active scanning and probing techniques may be inappropriate. It works by monitoring network traffic without directly interacting with devices. Imagine a network switch observing traffic patterns: it can see which devices are communicating, how frequently and using what protocols. Nozomi Networks' Guardian network sensors, in conjunction with remote collectors, are workhorses at passive discovery. They. continuously monitor the network to discover newly connected assets.

Active discovery

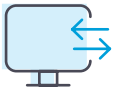
Passive discovery is tried and true, but it has limitations. It can't detect silent devices or those that aren't actively transmitting data. This means hidden risks can go undetected, such as dormant devices, rogue assets or misconfigured endpoints that aren't generating network traffic but still pose a security threat.

Active discovery fills in these blind spots. With a growing understanding that complete visibility is foundational to resilience, it's also becoming the norm in industrial networks.

Referred to as Smart Polling in the Nozomi Networks platform, active discovery probes the network, sending carefully crafted queries such as network pings or protocol-specific requests to devices. This is like a system administrator actively polling connected assets to ask, "What type of device are you?" "What services are you running?" Active querying reveals more details about devices, even those that aren't communicating, but must be done carefully to avoid disrupting critical operations.

Third-party integrations

Most OT/ICS environments rely on dozens of technology solutions, many of which capture valuable data that can be tapped to enrich asset inventories. The Nozomi Networks platform has a growing library of third-party connectors that can pull structured asset data from where it already exists, such as Microsoft Active Directory, Microsoft Defender, Cisco routers and switches, CrowdStrike, ServiceNow and other leading IT security solutions.



3. DPI and Protocol Coverage

The third thing to evaluate in an asset inventory solution is whether the data it collects is valuable to operators and security analysts. To troubleshoot In OT/IoT environments, you need a combination of deep packet inspection (DPI) and comprehensive protocol coverage to ensure you don't just see all your assets but understand what they're doing and who they're communicating with.

Deep packet inspection

Visibility into process variables and flows is essential for early anomaly detection. That can only be achieved using DPI to carefully analyze proprietary industrial protocols like Modbus or Profibus. Look for passive sensors purpose-built for OT networks that use DPI to automatically discover network components, connections and topology — and reveal threats.

Industrial protocol coverage

IT systems communicate using standard protocols, but OT systems use a wide range of protocols, many of them proprietary and industry specific.

Device profiles will always be incomplete if the solution can't analyze network traffic and asset-to-asset communications, key indicators for flagging potential issues in your environment. Since assets communicate via their protocols, fluency in a wide range of protocols is the key to understanding asset behavior. If your tool doesn't support a protocol, you're blind to those behaviors.

The Nozomi Networks platform understands hundreds of OT, IoT and IT protocols, from common to obscure, and we're constantly adding more. Using our protocol software development kit (SDK), we can quickly create new protocol support on demand.

4. Behavioral Baselining

AI and machine learning are essential for baselining asset behavior and detecting anomalies. Look for a system that employs AI to learn your environment and establish a baseline of “normal” behavior, then uses behavior analytics to monitor the network and alert on suspicious events.

AI-powered anomaly detection

Upon deployment in your environment, the Nozomi Networks platform begins monitoring device communications in “learning” mode, down to process-level variables. It uses AI to create detailed profiles of the expected behavior of every device at each stage in a process to establish a baseline of “normal” behavior.

When switched to “protection” mode, the platform uses behavior analytics to monitor the environment and alert on suspicious events that deviate from those baselines, while filtering out benign anomalous activity below established thresholds. In this way, asset behavior becomes an essential part of each asset profile..

5. AI Enrichment from Asset Intelligence

Keeping current with one or more targeted threat intelligence subscriptions is the best way to ensure you can detect known threats that may be in your environment.

Similarly, an asset intelligence feed that enriches sensor profiles by filling in missing information is the best way to ensure you’re current on all available data about your assets, giving you the most robust, accurate inventory possible.

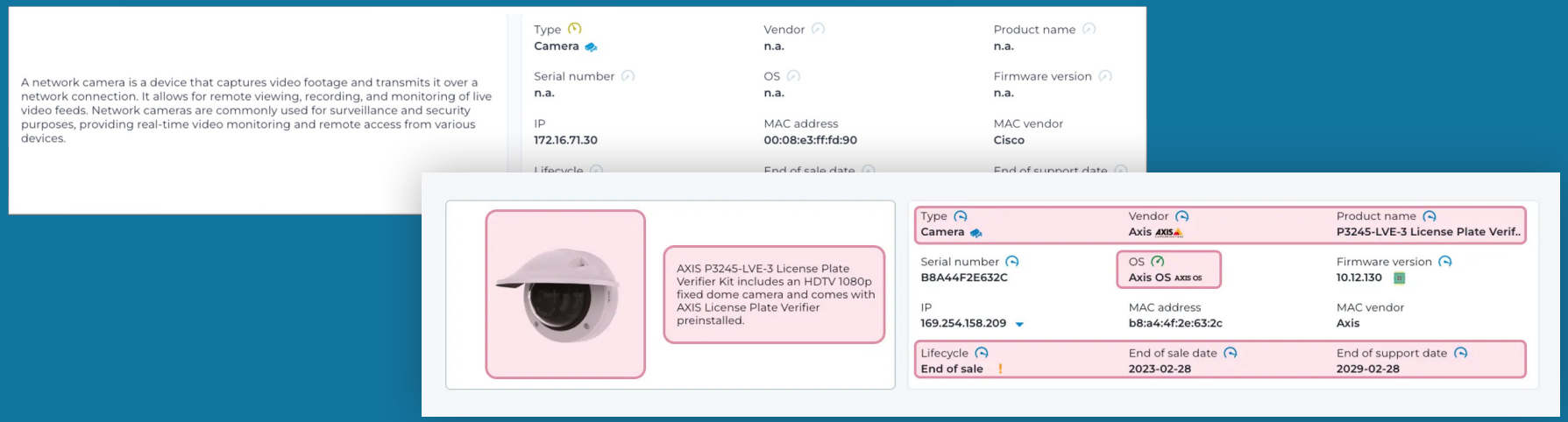
For this to add value in your environment, look for a vendor that community-sources anonymized customer asset data to populate asset profiles across its base — and whose customer base includes a sufficiently large number of organizations like yours to add value..

Achieve near 100% device classification accuracy with AI-enriched profiles

Available as a subscription, the Nozomi Asset Intelligence feed uses artificial intelligence curated by Nozomi Networks Labs data engineers to enrich device profiles with missing information including OS and firmware updates, product recalls, lifecycle status and known vulnerabilities, as well as expected function codes to understand normal behavior and help detect anomalies. These continuously updated profiles enable you to make informed decisions about the maintenance and security of your OT and IoT devices.

Our AI engine learns from millions of assets that we monitor in customer environments across industries around the globe.

This data is used to fill in gaps about identical devices across environments.. When a match is found, those attributes and behaviors are added to your device profile. The Nozomi Networks Labs team adds product images, descriptions to the database along with Common Platform Enumerations (CPEs), essential identifiers for accurately mapping vulnerabilities to assets in your environment and knowing which ones are important. The same data is used to determine known behavior, reducing the number of benign alerts by knowing when “new” or “different” isn’t a risk.



Asset profile before and after Asset Intelligence enrichment

Don’t Skimp on Asset Inventory, Your Cybersecurity Foundation

Industrial and critical infrastructure networks typically contain thousands of OT devices from hundreds of vendors, as well as IoT devices, that monitor and control processes. Creating an accurate, up-to-date inventory of these assets and keeping track of them, along with important context information, is foundational to cyber and operational resilience. It can’t be done manually.

Using a combination of endpoint-to-air sensors, passive and active data collection, OT/IoT protocol support and third-party IT asset data, the Nozomi Networks platform provides a complete asset inventory — turbocharged with actionable, AI-powered asset intelligence. When looking for and industrial asset inventory solution, that will help you advance on the cybersecurity maturity curve., consider Nozomi Networks as the gold standard.

Questions to Ask Vendors

1

What kind of sensors does your platform use for asset discovery and monitoring?

2

What data collection methods does your platform use?

3

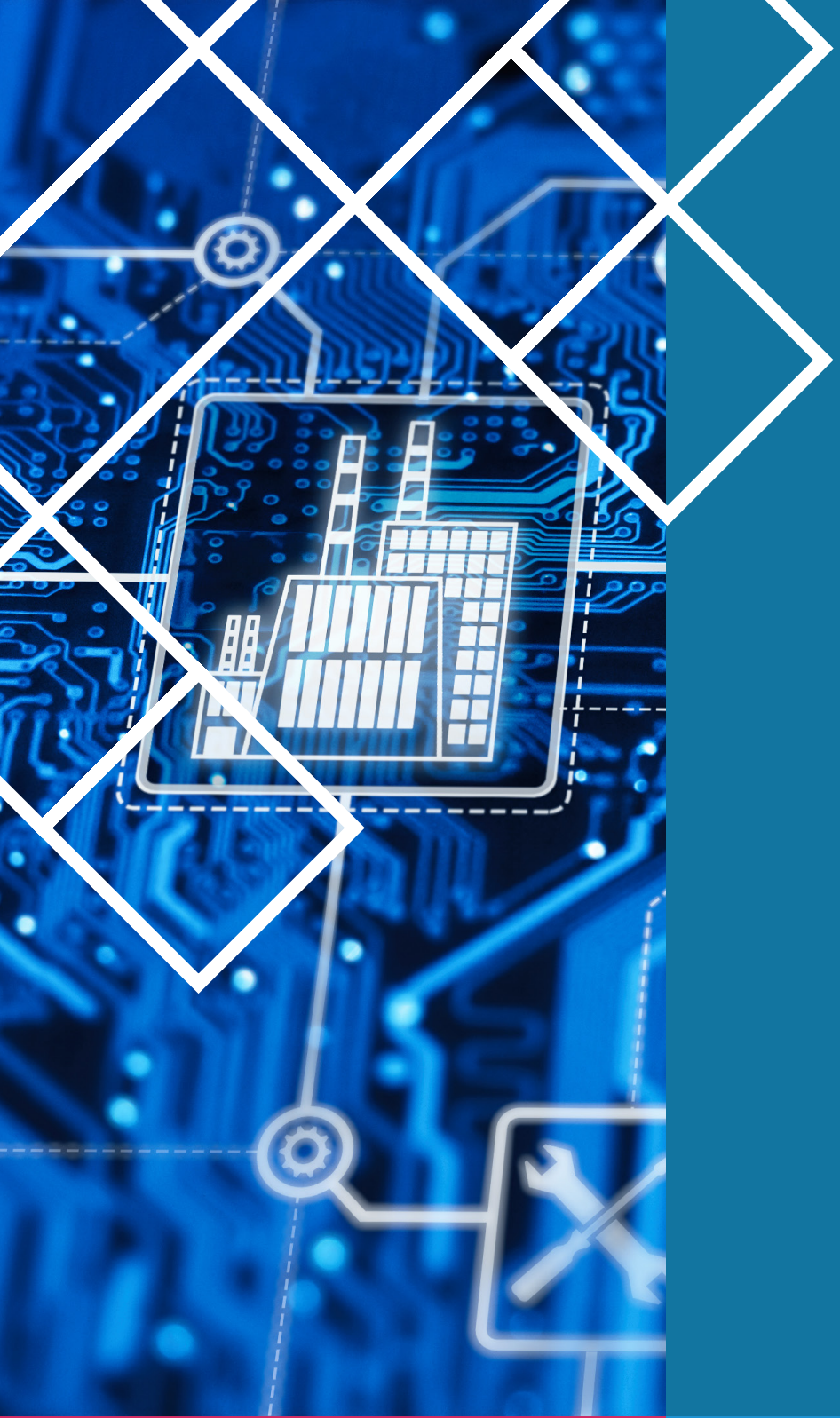
Does your solution use DPI to understand network traffic?

4

What OT, IoT and IT protocols does your solution understand?

5

How do you use AI and **machine learning**?



NOZOMI NETWORKS

NEXT STEPS

To learn more about how Nozomi Networks can help protect your OT/IoT systems, visit:

nozominetworks.com

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com