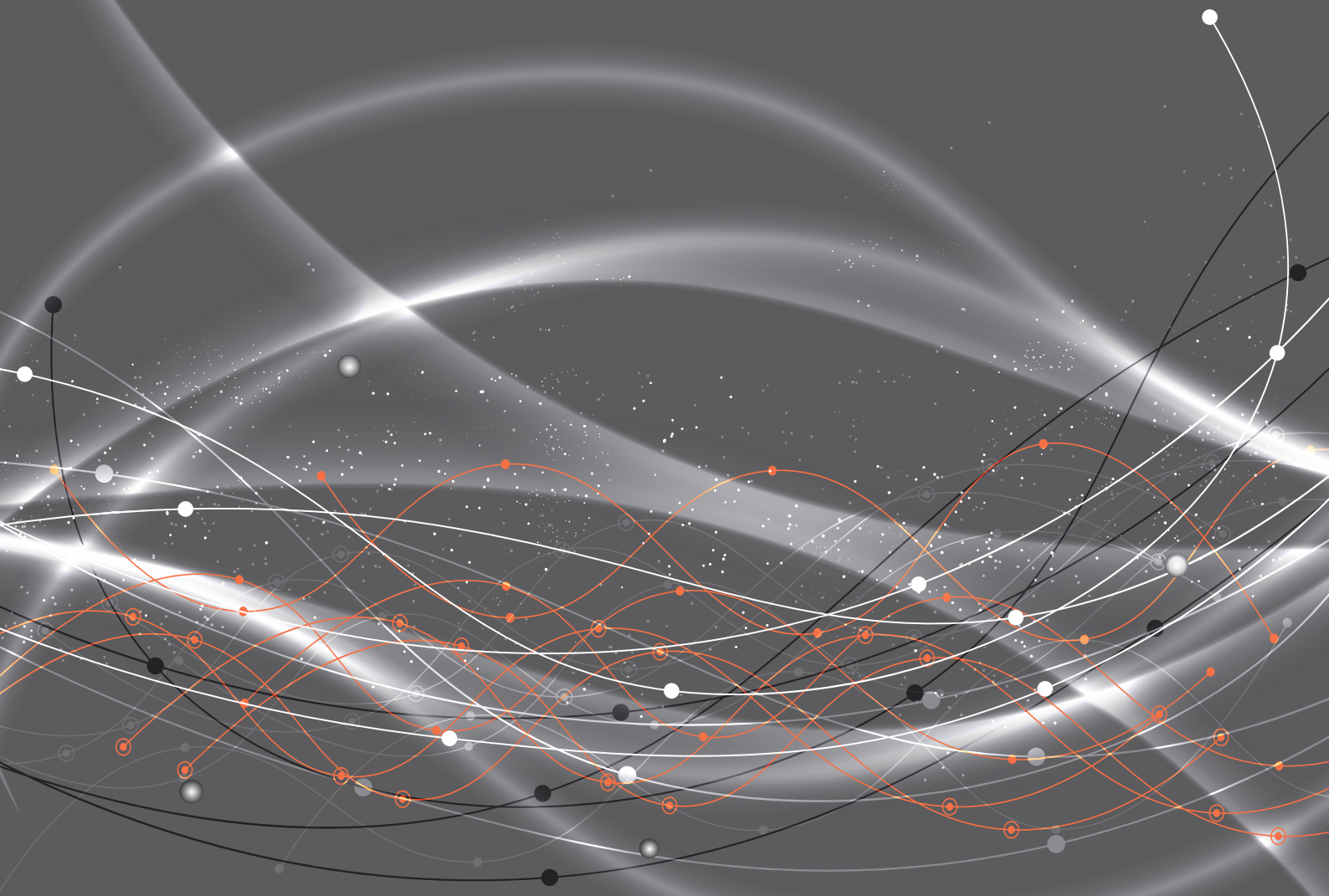
IXDen

IoT security that makes sense

Closing Critical Gaps in OT Cyber-Physical System Security and Data Health



If you're not protecting and analyzing your sensor data at the physical layer where it is generated, you cannot assure OT system cybersecurity or OT system data you can trust.

OT Sensor Layer versus OT Network Layer Protection

When cybersecurity monitoring is conducted at the network level, the SCADA system receives and processes a fraction (~20%) of sensor data. The vast majority of sensor data is handled by local controllers and never propagated upward. SCADA polling intervals can be from minutes to hours, depending on the industry and the process. For cybercriminals, a polling interval of 15 minutes is plenty of time to wreak havoc. Furthermore, much of the data sent to the SCADA system is not raw data from the sensor, but the data that is already processed. As such its veracity cannot be determined.

When cybersecurity monitoring is conducted at the physical sensor layer of the OT network, 100% of the sensor data is seen and analyzed in real-time by locally deployed agents. Most agent-based solutions analyze for anomalies per sensor or per parameter. Independent monitoring agents propagate all data directly from the sensor to a data processing server at the management level, greatly enhancing OT security and providing accurate visibility of OT data health.

Cybersecurity at physical Sensor layer	Cybersecurity at Network layer
Agent deployed at physical sensor/ controller Server deployed in the Data Center	Deployed in the Data Center
100% of sensor data propagated upward	~20% of sensor data propagated upward
Supports continuous data propagation	Data propagation to SCADA at intervals
All propagated sensor data is raw, transactional data	Most propagated sensor data is processed
100% of sensor transaction data available for AI analysis	Only a fraction of sensor data available for AI analysis
AI analysis and behavior modeling per: • sensor / parameter • parameter interdependencies	AI analysis and behavior modeling per parameter

Monitoring OT System Data Health

Sensor data that cannot be trusted poses a risk to the health of the OT system. It is a known phenomenon that industrial sensor data becomes less reliable over time. Misbehaving sensors send wrong measurements and wrong data that affects critical real-time decisions of local OT controllers, as well as management decisions regarding asset maintenance, replacement, refurbishment, etc. It is practically impossible to gauge the overall behavioral health of the OT network when only a fraction of sensor data is analyzed; when sensor data can't be trusted; and when sensor behaviors are analyzed in isolation from one another.

Protect OT Security and OT Data Health with one Agent-Based Solution from IXDen

IoT agent-based monitoring and analysis of sensor data and behavior is the answer to the OT Cyber and Operational conundrum. Agent deployment on physical assets no longer has to be perceived as complex and expensive. IXDen technology innovation has made it so much easier and cost-effective to protect OT system security and OT data reliability with one "protection at source" solution.

Protect the Veracity of OT Sensor Data at the Source

IXDen monitors sensor data where it is generated and leverages 100% of sensor transaction data for both security and health analysis. Only IXDen models single sensor behavior as well as multi-sensor interdependencies, enabling industrial enterprises to detect anomalies in flow as well as point behaviors, and to reduce false positive and false negative alerts.

Stop Sensor Data Manipulation and Data Injection Attacks

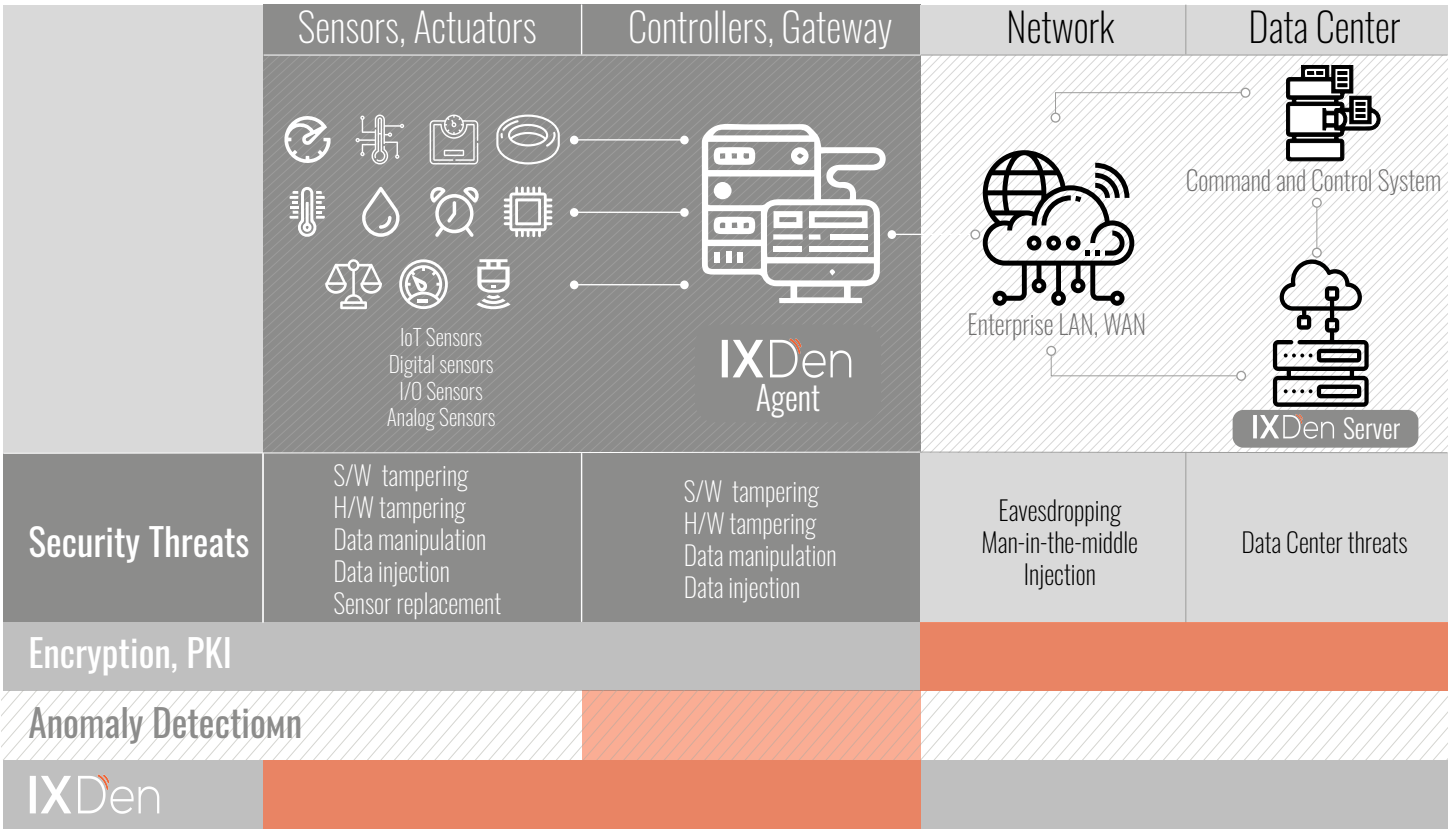
Cyberattacks are oftenpreceded by reconnaissance to determine the best way to inject or manipulate data. While the breach may occur at the cyber level, the results are felt at the physical level of the OT system and can be detected if you know what to look for. By monitoring sensor data at its source, discrepancies between IXDen data and manipulated sensor data sent to the SCADA will be detected immediately.

Accurately Gauge OT System Health

With 100% of transactional data coming in from sensors throughout the OT system, IXDen is able to analyze and evaluate the overall health and reliability of OT systems with extreme accuracy. IXDen innovation presents a single score that gives a general indication of sensor behavior and data health across the OT environment plus the ability to drill down to root causes.

IXDen Data-at-Source Protection Architecture Features:

- Non-intrusive IXDen SW agent deployment; no rewiring or instrumentation needed
- Passive operation; no impact on sensor/controller OS, application SW, functionality
- Powerful IXDen server in the data center with dashboard for analysis, alerts, health score
- Highly cost effective; complements network-based OT Security solutions



Protect OT Sensor Data at Source

Contact IXDen to learn how software-only, IoT agent-based cyber-physical solutions can bring better OT security, better OT system health, and peace of mind to your industrial OT environment.